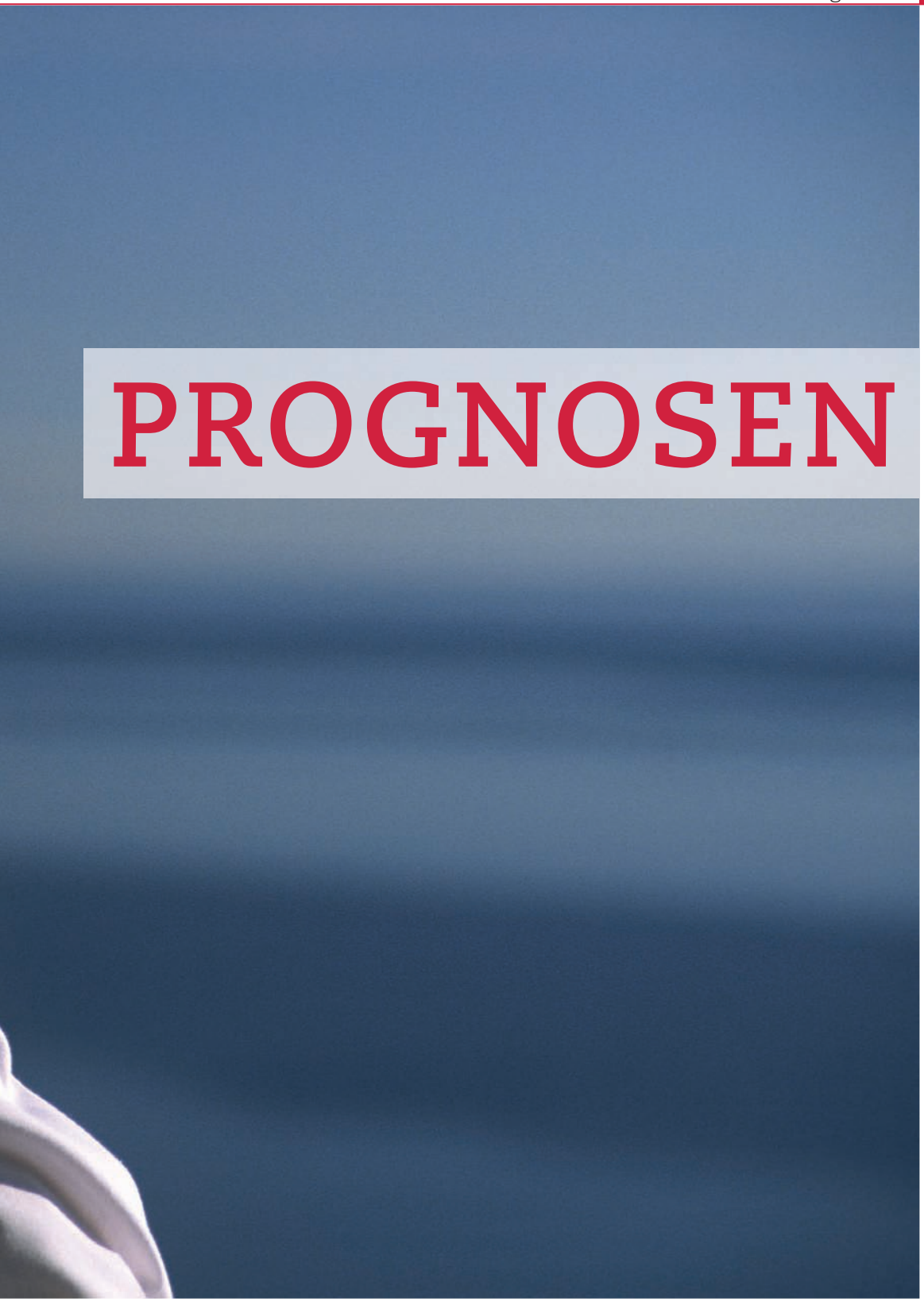

PROGNOSEN

DAS INTERNET IST REIF FÜR DIE INSEL

Guus Dekkers, CIO Airbus & Corp. CIO EADS

„Ich wette, das sich das heutige Internet in zehn Jahren in viele Einzel-Inseln aufgelöst hat."

Schön war die Zeit, als Cyber-Probleme lediglich in den CIO-Kreisen und deren Fachblättern diskutiert wurden. Cyber-Zwischenfälle stellten damals zwar ein ärgerliches Thema für jeden CIO dar, waren aber irgendwie dann doch beherrschbar und ohne große Sichtbarkeit und nachhaltige Auswirkungen. Auch wenn wir vielleicht alle gehofft hatten, dass dies so bleiben würde, sind wir leider in den vergangenen Jahren schmerzvoll eines Besseren belehrt worden.

Heute vergeht fast kein Tag, an dem nicht auch Mainstream-Medien wie die Tagespresse und die populären Nachrichtenmagazine sich gehalten sehen, über Cyber-Auswüchse zu berichten, und das mit immer alarmierenderen Botschaften. Cyber-Kriminalität ist mittlerweile ein eminent präsentes Thema in der öffentlichen Wahrnehmung und Meinungsbildung geworden, in der vor allem die Überraschung über die Dimension dieser kriminellen Aktivitäten, deren potenziell zerstörende Wirkung auf unseren gesamten Rechtsstaat sowie die gefühlte Hilflosigkeit gegen derartige Attacken vorherrscht.

Auch wenn die ersten beiden Punkte die CIO-Community sicherlich nicht recht überraschen, entwickelt sich das dritte Thema immer mehr zu einem Problemfall. Die Korrekturmöglichkeiten des Rechtsstaates zu diesem Thema erscheinen zurzeit eher limitiert und fokussieren sich – zumindest in der öffentlichen Wahrnehmung – zuerst einmal primär auf die Durchsetzung von (nationalen) Urheberrechtsansprüchen, eine Maßnahme, die aktuell bekanntermaßen sehr intensiv und ausgesprochen kontrovers diskutiert wird. Dies wirbelt zwar viel Staub auf und wird sicherlich letztendlich auch zu einer Anpassung des Urheberrechts an die neuen technischen Gegebenheiten führen, ist aber im Kontext der – professionellen – Internet-Kriminalität eigentlich nur als zweitrangig anzusehen. Für die CIO-Gemeinschaft ist sie damit allein insofern interessant, als man selbstverständlich die notwendigen Maßnahmen ergreift, um das eigene Unternehmen hinsichtlich potenzieller Verstöße gegen das Urheberrecht abzusichern.

Zweitrangig ist diese Quasi-Gegenmaßnahme vor allem deshalb, weil derartige Verfahren le-

diglich dazu taugen, Individuen zum Zweck der Durchsetzung von Urheberansprüchen adressieren zu können – und auch hier meistens noch limitiert auf den nationalen Rahmen. Der professionell agierende Internet-Kriminelle, der eindeutig viel größeren volkswirtschaftlichen Schaden anrichtet, wird jedoch vom Wirkungskreis derartiger Maßnahmen nicht erreicht. Aufgrund seines undurchsichtigen Operationsterrains, seiner professionellen Organisation und Vorgehensweise sowie der internationalen Verflechtungen ist ihm mit den anwendbaren Rechtsmitteln der Bundesrepublik Deutschland nicht hinreichend beizukommen.

Aus volkswirtschaftlicher Sicht drängt sich so die Einschätzung auf, dass man leider eher auf unzulängliche, wenn nicht gar ungeeignete Mittel zur Eindämmung derartiger Internet-Kriminalität setzt: Die in diesem Umfeld spärlich verfügbaren Experten, Ressourcen und finanziellen Mittel werden im großen Stil für die Entgegnung individueller Urheberrechtsverletzungen und anderer recht gut einzugrenzender Straftaten im Internet-Raum eingesetzt und mögen ja hier durchaus zu einem effizienten Ergebnis beitragen und obendrein Heerscharen von Anwälten einen erklecklichen Umsatz bescheren. Das aber ist eben sowohl im Einzelnen als auch in Summe bei Weitem zu wenig und nicht effektiv genug, um die Gesellschaft grundsätzlich gegen international verästelte, professionelle Internet-Kriminalität zu schützen. Die CIO-Gemeinschaft wird damit immer mehr gezwungen, selbst geeignete Maßnahmen zur Abwehr derartiger Vorgehensweisen zu treffen. Wer wünscht sich da nicht insgeheim doch die Abkehr von der weltumspannenden Internet-Cloud und stattdessen das private Glück auf einer kleinen, geschützten Internet-Insel in einer Art lockerem Insel-Commonwealth …

So scheint es, dass sich trotz all unserer gemeinsamen Bemühungen das Internet immer mehr zu einem durchweg anarchistischen Raum transformiert (hat) – Anarchie im Sinne von einem „durch die Abwesenheit von Staat und institutioneller Gewalt bedingten Zustand gesellschaftlicher Unordnung, Gewaltherrschaft und Gesetzlosigkeit“ (Deutsche Wikipedia). Und da sich die professionell agierenden Internet-Kriminellen von wirksamen und effektiven Regulierungs- und Überwachungsmaßnahmen weitestgehend verschont sehen und so ihre Straftaten meistenteils unbehelligt betreiben können, wird dieses „Geschäftsgebiet“ kontinuierlich lukrativer, und die Ausführenden werden immer dreister und einfallsreicher.

Das Internet als anarchistischer Raum

Letztendlich wird dieser Missstand nach meiner Meinung zu einem Zustand führen, in dem man im Internet nichts und niemandem mehr so wirklich vertrauen kann. Dieser Zustand wird dann nicht nur die professionelle CIO-Gemeinschaft betreffen, sondern natürlich auch jeden von uns in seiner privaten Internet-Nutzung, weil auch die massenhaft betriebene „Kleinkriminalität“ den Tätern immer attraktiver und einfacher erscheint.

Also bleibt uns nichts anders übrig, als uns selbst zu schützen, was zur Einführung von immer raffinierteren Filtern, Scannern und Verfahren führt, um die Spreu vom Weizen trennen zu können und so nur mit Partnern zu kommunizieren, von denen wir glauben, ihnen auch wirklich vertrauen zu können. E-Mails werden gefiltert und gegebenenfalls eliminiert, dubiose Websites mittels „black/white listing“ ausgeschlossen und die Virenscan-Datenbanken immer umfangreicher – und doch scheinen wir das Wettrennen wegen der schieren Masse der möglichen Kommunikationspartner, der Vielfalt der Kommunikationsmöglichkeiten und der Raffiniertheit des kriminellen Gegenübers – der nur einen Day-0-Exploit braucht, um zu siegen, während wir alles und jeden kennen müssen, um uns wirklich wirksam schützen zu können – erstmals zu verlieren.

Also werden die Ungewissheiten, die uns treiben und umtreiben, immer umfangreicher: Wie kann ich dann in einem elektronischen Datenaustausch auch sicher sein, dass mein Partner, dem ich glaube trauen zu können, auch wirklich dieser Partner ist? Woher weiß ich, dass die Website, die ich soeben aufgerufen habe, auch wirklich von meiner Bank ist und keine Vortäuschung? Kann ich verifizierbar feststellen, dass die erhaltene E-Mail auch tatsächlich von demjenigen kommt, dessen Namen ausgewiesen ist? Und wie kann ich zuverlässig vermeiden, dass mein Datenaustausch (Stichwort: PIN-Code) auch wirklich nicht durch jemanden abgeschöpft und ausgenutzt wird? Die besten Filter und Verfahren der Welt werden nicht helfen können, wenn die Parteien, von denen wir meinen, ihnen trauen zu können, von der Cyber-Kriminalität unterwandert und missbraucht werden. Und genau dort setzen die fortschrittlichsten Cyber-Kriminellen bereits heute an.

Ohne Kontrolle kein Vertrauen

Die Voraussetzungen für einen vertrauensvollen Austausch werden also vielfältig: Erstens muss ich meinem Kommunikationspartner als „physischer/moralischer" Person überhaupt vertrauen. Zweitens muss ich davon ausgehen können, dass seine Kommunikationsverfahren nicht durch Fremde unterwandert wurden. Drittens darf der Kommunikationsaustausch – zumeist über das Internet – selbstverständlich nicht korrumpiert werden. Und viertens muss ich meiner eigenen EDV angemessen vertrauen können. Während die meisten CIOs – und auch Privatanwender – glauben, den ersten und letzten Punkt hinreichend beantworten zu können, ist das Problem bezüglich der Aspekte zwei und drei weitaus komplizierter.

Da wir es lediglich mit einem elektronischen Abbild des Kommunikationspartners zu tun haben, kann nur dieses „Virtual Picture" für die Beantwortung der Vertrauensfrage herangezogen werden. Es muss also etwas enthalten, das es dem Empfänger ermöglicht, die Vertrauenswürdigkeit des beabsichtigten Datenaustauschs zu prüfen. Dies baut auf verbindliche und geschützte Absprachen auf, die nur Partner, die diesem Kreis angehören, einhalten und vorzeigen können. Vertraut wird dann meistens nur, wenn der Datenaustausch – unabhängig davon, ob E-Mail, Website oder anderer Content – eindeutige Merkmale aufweist, zum Beispiel auf eine bestimmte Art und Weise verschlüsselt wurde ‚oder bestimmte Zertifikate aufweist. Das Prinzip ist also einfach: Merkmal vorhanden, dann vertraue ich dir und lasse die Kommunikation zu, falls nicht, dann bleibt meine Tür für dich verschlossen.

Damit dieses Konzept zuverlässig funktioniert, ist es also wichtig, dass nur der „vertraute Kreis" in der Lage ist, die Merkmale zu beurteilen und gegebenenfalls auch zu erstellen. Genauso wichtig dabei ist selbstverständlich auch, dass nicht zu dem Kreis gehörende Teilnehmer – hier ist natürlich vor allem die Hacker-Gemeinde gemeint – dies nicht können. Es muss ihnen also vor allem unmöglich sein, die geschützten Sicherheitsmerkmale erstellen, reproduzieren oder unterwandern zu können. Sobald ihnen das nämlich gelingt, ist die Schutzwirkung des Verfahrens hinfällig.

Die skizzierte Methode ist ja an sich nichts Neues, bereits heute werden viele derartige Verfahren angewandt, um oben genannte Vertrauensfrage einigermaßen zuverlässig beantworten zu können. Gute Beispiele sind die Bankenverschlüsselungsmodelle HBCI oder das PGP-E-Mail-Verschlüsselungsverfahren sowie das zertifikatsbasierte Prüfungssystem nach dem europäischen Abkommen SOGIS-MRA V3.

Wenn wir aber die immer weiter zunehmende Notwendigkeit und Akzeptanz der Einführung derartiger Verfahren akzeptieren, wird das weitreichende Folgen für das Internet haben. Das World Wide Web, die weltumspannende Internet-Wolke, wird gleichsam realiter in einen Zustand überführt, den man mit der Co-Existenz zahlreicher Internet-Einzelinseln beschreiben kann.

Wie es zu diesen Einzelinseln kommen wird? Erstens lässt sich aus dem genannten (Un-)Sicherheitstrend sicherlich extrapolieren, dass wir in einiger Zeit wirklich nur noch mit Partnern kommunizieren, bei denen wir meinen, ihnen dank eines der skizzierten Sicherheitsmechanismen trauen zu können. Die Unsicherheiten und Sicherheitsrisiken bei einem „nicht geprüften Partner" werden schlichtweg so hoch, dass sich die CIOs – und ultimativ auch die Privathaushalte – nicht mehr an einen derartigen Kommunikationsaustausch wagen werden. Daraus folgt: kein Vertrauensmerkmal = kein Kommunikationspartner.

Ein einziges Trust-Verfahren wäre nicht vertrauenswürdig

Zweitens wird es unwahrscheinlich sein, dass es nur ein einziges elektronisches Vertrauensmerkmal geben wird, so wie es zum Beispiel die deutsche Bundesregierung in ihrem Zukunftsprojekt „Sichere Identitäten" vorantreiben möchte. Die Unwahrscheinlich rührt aus markanten Gründen: Zum einen hat sich die Fähigkeit der IT-Industrie, Einigkeit in Fragen verbindlicher weltweiter Standards zu erzielen, in der Vergangenheit als unzureichend herausgestellt. Zum anderen könnte sich ein singuläres Vertrauensmerkmal auf Dauer nicht der Unterwanderungsambitionen erwehren, wie etwa die massiven Versuche, das HTTPS-Protokoll zu knacken, eindeutig belegen. Daraus folgt: Würde ich mich nur einem Verfahren anschließen, wären meine Kommunikationsmöglichkeiten zwangsläufig nur auf die zu diesem Kreis gehörenden Partner beschränkt. Die anderen Partner würden außen vor bleiben.

Drittens bauen derartige Verfahren immer darauf auf, dass ich dem „Ur-Inhaber" des Verfahrens tatsächlich vertrauen kann. Auch unter Nichtberücksichtigung eventuell national getriebener Interessen – etwa die anzunehmende Möglichkeit, dass ein Verfahren, das seinen Ursprung in einem bestimmten Land hat, auch durch irgendeine oder mehrere Behörden dieses Landes unterwandert wurde – machen zwei Beobachtungen die Grenzen der Benutzung und Vertraulichkeit solcher Methoden offensichtlich.

Neben das bereits oben angeführte Argument, dass schiere Größe gleichsam automatisch bestimmte kriminelle Kreise motiviert und auf den Plan ruft, tritt folgender Sachverhalt: Ein „Ur-Inhaber" kann bei immer wachsenden Anwendungsumfängen kaum mehr sicherstellen, dass jegliche Benutzer sämtlichen Anforderungen zur Benutzung dieses Verfahrens kontinuierlich entsprechen. Der Prüfungsaufwand wäre schlichtweg zu hoch, und die Teilnehmer wären zu anonym und damit zu unbekannt. Obendrein ist das statistische Risiko, dass ein Teilnehmer dann doch unterwandert wurde oder ganz einfach „falsche Absichten" verfolgt, bei einem zu großen Kreis tatsächlich um ein Vielfaches höher. Daraus folgt: Je größer der Anwendungskreis des Verfahrens, umso unsicherer wird es.

Das wiederum bedingt: Für unterschiedliche Sicherheitsfragen werden wir unterschiedliche Verfahren einsetzen (müssen). Und letztendlich: Da es sehr unwahrscheinlich ist, dass sämtliche meiner Kommunikationspartner nur einem Kreis angehören, werde ich mich zwangsläufig mehreren Kommunikationskreisen anschließen müssen.

Die Wette gilt: In zehn Jahren sehen wir auf ein Internet, das zwar das Internet-Protokoll noch als „rohes Transportmedium" für Datentransport benutzt, aber durch die Aufteilung in abgeschlossene Nutzergruppen de facto in eine Unmenge von Inseln zerlegt ist.

Und wir werden auf jeden Fall viele dieser Internet-Inseln besuchen, vielleicht aber dann doch nicht alle. Wird da noch etwas Gemeinsamkeit sein mit dem Traum vom glücklichen Inseldasein? Wir werden sehen ...

Ich freue mich auf Ihre Gegenwette!

premium.cio.de/cio-netzwerk/profil/guus-dekkers

BIS 2023 WIRD'S NIX MIT „ZERO E-MAIL"

Martin Gnass, CIO der Hapag-Lloyd AG

„Ich wette, dass auch in zehn Jahren der überwiegende Anteil der geschäftlichen elektronischen Kommunikation per E-Mail erfolgen wird."

Erstens kommt es anders, und zweitens, als man denkt", sagt der Volksmund. Oft genug trifft dies auch für IT-Prognosen zu. Auch wenn die IT-Vorhersagen selbst ernannter Marktauguren oft genug falsch liegen, wage ich einen Blick in die „IT-Glaskugel 2023" für folgende Themenbereiche:

Zentralisierung von Informations-Services

Für weltweit agierende Unternehmen, deren Geschäftsprozessmodell einem hohen Grad an Standardisierung unterliegt, ist die zentrale Bereitstellung von IT-Infrastruktur- und Applikations-Services für die globale Organisation „aus der Netzsteckdose" per MPLS-Netz beziehungsweise Internet übliche Praxis. Darüber hinaus sind in vielen Unternehmen noch „lokale" Systeme und Datenhaltung auf File-Servern in den Büros beziehungsweise Niederlassungen anzutreffen. Diese Services werden künftig eine weitgehende Zentralisierung erfahren.

Der Consumer-Bereich ist in vielen Dingen Vorreiter. Tradierte Konzepte für lokale Datenspeicherung werden durch zentrale Data-Services abgelöst. Apples Cloud Service, Drop Box und weitere werden Nachahmer finden, die ein sicheres und – im Gegensatz zu Apple – ein produkt- respektive plattformneutrales Daten-Hosting ermöglichen. Consumer werden künftig auf einfache Art und Weise mit beliebigen Endgeräten auf ihre Daten zugreifen und sicher(er) als heute archivieren können. Im privaten Bereich wird in zehn Jahren (hoffentlich) kein Anwender mehr „Hand-am-Arm"-Daten per USB-Stick von A nach B kopieren und sich um das Backup seiner privaten PC- und Notebook-Festplatten kümmern müssen.

Im Unternehmen wird künftig die „Enterprise Cloud" abteilungsspezifische fachliche Anwendungen und Daten als zentralen Service bereitstellen. Standortspezifische Datenhaltung auf File-Servern, Laufwerkverzeichnisse und so weiter werden durch diese zentralen Data-Services abgelöst sein.

Die Zentralisierung der Informations-Services hat neben den bekannten technischen und kommerziellen Vorteilen auch positive Effekte für die

Agilität von Unternehmen: Organisatorische Veränderungen werden schneller unterstützt und IT-seitig abgebildet, da Netzzugang und Endgeräte als Zugangsvoraussetzung schnell bereitgestellt werden. Beispiele: Post Merger Integration, das Bündeln von Tätigkeiten in „Shared Services"-Teams, Umsetzung von Restrukturierungsmaßnahmen. Auch Business-Continuity-Konzepte können IT-seitig durch die „Enterprise Cloud" besser unterstützt werden.

Fazit: In zehn Jahren wird lokale Daten- und Applikationshaltung weitgehend Geschichte sein. Der bereits in den 90er-Jahren beworbene „IT-Service aus der Steckdose" ist endlich Wirklichkeit geworden.

Veränderung von Arbeitsformen und Arbeitswelten

Moderne ITK-Konzepte und breitbandige Internetverbindungen ermöglichen seit etlichen Jahren die Flexibilisierung der Arbeitswelten und das weitgehend ortsunabhängige Arbeiten. Der Adaptionsgrad „virtualisierter Arbeitswelten" ist jedoch firmen- und branchenabhängig sehr unterschiedlich.

Ein Paradebeispiel sind die Unternehmen der IT-Dienstleistungs-/Beratungsbranche, die seit Jahren flexible Modelle zur Arbeitszeit- und Arbeitsplatzsouveränität eingeführt haben (Home-Office- und Shared-Office-Konzepte). In anderen Branchen und Unternehmen ist dies jedoch noch die Ausnahme beziehungsweise auf einzelne Mitarbeiter beschränkt.

Eine repräsentative Umfrage des Branchenverbandes Bitkom 2010 ergab, dass zehn Prozent der Berufstätigen in Deutschland ganz oder teilweise von zu Hause arbeiten. Der Office 21 Forecast des Fraunhofer-Instituts für 2024 besagt, dass für 94 Prozent der Befragten eine hohe Flexibilität bei der Wahl des täglichen Arbeitsortes die Regel sein wird. Wie geht der Trend nun weiter? Ist in zehn Jahren das klassische Firmenbüro überflüssig geworden und damit der IT-Arbeitsplatz im Büro ein Auslaufmodell und durch BYOD abgelöst?

Meine Prognose: So wird es – zumindest flächendeckend – nicht sein. Unbestritten werden demografischer Wandel, gesteigerte Work-Life-Balance-Erwartungen qualifizierter Mitarbeiter in den entwickelten Gesellschaften sowie Verkehrsinfrastrukturprobleme die Flexibilisierung der Arbeits- und Lebensbedingungen vorantreiben. Gleichwohl laufen Veränderungsprozesse hinsichtlich der Organisation von Arbeit nach unterschiedlichen Maßstäben – und in Deutschland und Europa tendenziell eher langsam – ab. Die Flexibilisierung der Arbeit durch Mobilitätskonzepte wird zudem in Teilen von Management- und Mitbestimmungsgremien zurückhaltend behandelt. Auch bei Mitarbei-

tern ist die Euphorie unterschiedlich groß. Die bekannten Gründe: Angst vor Steuerungs- und Kontrollverlust, Verlust des Identifikationsbeziehungsweise Zugehörigkeitsgefühls zum Unternehmen, Angst vor dem Verlust sozialer Kontakte.

Meine Erwartung: Arbeitszeit- und Arbeitsplatzsouveränität werden in den nächsten Jahren moderat zunehmen und „virtuelle Belegschaften" in der Minderheit bleiben. Dies hat auch für die IT Konsequenzen: Der klassische Büroarbeitsplatz ist in zehn Jahren noch nicht passé. Die Unternehmens-IT wird auch künftig IT-Arbeitsplätze anbieten, die den Prinzipien der Standardisierung, Kosteneffizienz und Zuverlässigkeit unterliegen. Dies wird nicht mehr der PC/Desktop sein, sondern Techniken wie Thin Client, VDI-basierte Konzeptmodelle oder Ähnliches.

Mobilität wird für bestimmte Mitarbeitergruppen weiter zunehmen, BYOD für mobile „Smart Worker" Einzug halten. Unabhängig davon werden Teile des Managements, Mitbestimmungsgremien und Mitarbeiter nach wie vor erwarten, dass das Unternehmen mobile Arbeitsgeräte zur Verfügung stellt.

Bekanntlich entwickeln sich die Möglichkeiten der digitalen Zusammenarbeit rasant weiter. Digitale Medien („Social Media") finden zunehmende Verbreitung im privaten und beruflichen Umfeld. Daraus ergeben sich für die Unternehmen viele Chancen und Risiken. Der Grad der Adaption wird auch hier – in Abhängigkeit von Branche und Unternehmenskultur – unterschiedlich bleiben.

„Zero E-Mail" nicht in den nächsten zehn Jahren

Eine bekannte IT-Beratungsfirma ist früh auf das Thema aufgesprungen und hat bereits vor einem Jahr auf der CeBIT öffentlichkeitswirksam die „Zero E-Mail" für die Zeit nach 2015 proklamiert. Meine Prognose lautet: So wird es nicht sein. „Erprobte" Technologien haben eine längere Lebensdauer als oftmals angenommen; dies gilt auch in der ITK-Branche. Selbst die seit Langem totgesagte Faxtechnik ist (leider) immer noch im Arbeitsalltag existent.

Deshalb bin ich sicher: Auch 2023 hat die E-Mail noch einen hohen Stellenwert in der digitalen Kommunikation. Der überwiegende Anteil der geschäftlichen elektronischen Kommunikation wird noch per E-Mail erfolgen.

Ich freue mich auf Ihre Gegenwette!

Kontakt: http://premium.cio.de/cio-netzwerk/profil/martin-gnass