MEDIA PLANET

SEPTEMBER 2009

IT-SECURITY

Eine Zeitung produziert von Mediaplanet

MEDIA PLANET

Kriminelle Jagd auf Ihre Daten

Dr. Udo Helmbrecht,
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Liebe Leserinnen und Leser,

wissen Sie, was Ihre Identität wert ist? Auch wenn Sie sich darüber noch nie Gedanken gemacht haben sollten, Cyberkriminelle haben längst eine klare Vorstellung davon: Nach der Studie eines IT-Sicherheitsunternehmens ist die gestohlene Identität eines EU-Bürgers rund sechs US-Dollar wert – bei Abnahme von zehn Stück.

Das Beispiel zeigt: Die Computerkriminalität hat mittlerweile ein erschreckend professionelles Niveau erreicht. Längst sind hier keine geltungssüchtigen Einzeltäter mehr am Werk, sondern eine arbeitsteilig organisierte Schattenwirtschaft, die international operiert: Die einen stehlen Daten und bieten sie online auf Handelsplattformen an. Ihre kriminellen Kunden nutzen das digitale Diebesgut für betrügerische Geschäfte oder um Online-Bankkonten auszuplündern. Ein Milliardenmarkt, mit steigender Tendenz.

Hinzu kommt die immer größere Raffinesse der Angriffe. Längst haben die plumpen Phishing-E-Mails ausgedient, mit denen die Täter an die TANs von Bankkunden heran kommen wollten. Heute nutzen IT-Kriminelle Schwachstellen in Browsern und ihren Hilfsprogrammen als Einfallstore in die Computer ihrer Opfer. So gelangt die schädliche Software auf den PC, ohne dass der Nutzer etwas bemerkt.

Neue technische Entwicklungen werfen zusätzliche Fragen auf: Wie gut sind Daten geschützt, wenn sie künftig im Internet in einer „Computerwolke" gespeichert werden und der eigene PC nur noch als Zugangsgerät genutzt wird? Immerhin arbeiten IT-Experten daran, Cloud Computing auch für die Abwehr von schädlichen Programmen einzusetzen („Cloud Security"), weil herkömmliche Ansätze immer mehr an ihre Grenzen stoßen.

Erfreulich ist, dass das Sicherheitsbewusstsein der Nutzer parallel zur wachsenden Bedrohung steigt – Virenscanner und Firewalls gehören weitgehend zur Grundausstattung. Doch auch sie bieten keinen hundertprozentigen Schutz mehr. Jeder Nutzer ist daher aufgefordert, sich mit Vorsicht durchs Internet zu bewegen und sich umfassend zu informieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist nicht nur der zentrale IT-Sicherheitsdienstleister des Bundes – wir richten uns auch an Unternehmen und private Nutzer. Unsere regelmäßigen Lageberichte zur IT-Sicherheit informieren über aktuelle Bedrohungen (www.bsi.de). Unser IT-Grundschutz stellt Behörden und Unternehmen seit 15 Jahren bewährte Methoden zur Verfügung, um ihre Informationen effektiv zu schützen. Und unter www.bsi-fuer-buerger.de können sich Privatanwender über alle Aspekte der IT-Sicherheit informieren.

Mit der wachsenden IT-Kriminalität steigt das Risiko, zum Opfer zu werden. Machen Sie es den Tätern so schwer wie möglich, indem Sie Ihre wertvollen Daten bestmöglich schützen.

IT-SECURITY

Inhalt

MEDIA PLANET
MIT DER REICHWEITE EINER TAGESZEITUNG UND DEM FOKUS EINER FACHZEITSCHRIFT
www.mediaplanet.com

Mediaplanet Deutschland GmbH
Kurfürstendamm 177
10707 Berlin, Deutschland

IT SECURITY
PRODUZIERT VON MEDIAPLANET

Projektleiter: Dennis Ronneberger verantwortlich für Projektmanagement und Anzeigen, + 49 (0)30 887 11 29 40
Produktion/Layout: Jana Weiz
Business Development: Benjamin Römer, + 49 (0)30 887 11 29 35

Fotos: istockphoto.com
Text: Anna Katharina Fricke, Dr. Rainer Baumgart, Ivonne Thomas, Michael Menzel, Sarah Wagner Christoph Busch
V.i.s.d.P.: Christian Züllig, Print Director, Mediaplanet
Druck: Frankfurter Societätsdruck, Frankfurt

Mediaplanet ist die führende europäische Medienfirma, spezialisiert auf die Produktion, Finanzierung und Distribution von Themenzeitungen in der Tages- und Wirtschaftspresse.
Für weitere Informationen rufen Sie bitte Christian Züllig an, +49 (0)30 887 11 29 12

Auch in der Cloud lassen sich sensible Firmendaten wirksam schützen

Die Wolke ist sicher

Finger weg vom Cloud Computing? Viele Unternehmen scheuen den Schritt hin zu bedarfsorientierten und kostenvariablen IT-Ressourcen. Sie fürchten, dass ihre Informationen in fremde Hände geraten oder ihre Verfügbarkeit leidet. Spezialisierte Dienstleister bekommen die Risiken mit eigenen Wolken in den Griff.

VON DIPL.-ING. RENÉ REUTTER, CISSP, Abteilungsleiter, verantwortet bei T-Systems die Konzeption, Betrieb und die kontinuierliche Weiterentwicklung der Security Services & Solutions.

Die Marktforscher von Forrester Research und die Information Technology Intelligence Corp. (ITIC) kamen 2009 in zwei voneinander unabhängigen Studien zum gleichen Ergebnis: Akzeptanz und Nachfrage von Unternehmen halten sich beim Cloud Computing bislang in Grenzen. Ein Grund hierfür sind starke Sicherheitsbedenken. Laut der ITIC-Untersuchung verlangen 83 Prozent von weltweit 300 befragten Firmen mit bis zu 100.000 Mitarbeitern vor dem Schritt in die Wolke Garantien für den Schutz ihrer Daten. In sogenannten „Public Clouds", die über das öffentliche Internet laufen, ist das jedoch nicht zu realisieren.

Nur „private" ist privat

Damit aus der Wolke kein Orkan wird, brauchen Unternehmen einen Mix aus neuen Schutzfunktionen für die Cloud und im klassischen Outsourcing bewährten Sicherheitsstrategien. Kombiniert mit einer Anbindung ans Rechenzentrum eines ICT-Dienstleisters fließen Informationen über ein getunneltes Netz und nicht mehr über das öffentliche Internet. In einer derart virtualisierten Umgebung behält der Kunde vollständig die Datenhoheit.

In der privaten Wolke profitiert ein Unternehmen außerdem unmittelbar vom Security-Know-how des Providers. Hunderte von Experten beschäftigen sich täglich ausschließlich mit der Vermeidung von Attacken jeglicher Art beziehungsweise der richtigen Reaktion darauf. Für ein Unternehmen, das sich mit hochgradig ausgebildeten Angreifern im Netz herumschlagen muss, macht sich das schnell bezahlt. Darüber hinaus erbringen große ICT-Anbieter gleiche Leistungen für eine Vielzahl von Kunden und können durch die sich daraus ergebenden Skaleneffekte Technologien einsetzen, die es sich alleine kaum leisten kann. Selbst mobile Endgeräte wie Laptops, PDAs oder Smartphones und die mit ihnen abgebildeten Workflows lassen sich sicher in die Cloud integrieren

Maßnahmen angepasst an die Risikosituation

Im ersten Schritt in die Wolke müssen sich Unternehmen und Dienstleister über das nötige Sicherheitsniveau austauschen. Der ICT-Spezialist muss seinem Kunden die vorhandenen Risiken darlegen und ihn darüber informieren, was er gegen sie unternehmen kann. Das Stopfen von neu auftretenden Sicherheitslücken reicht im Cloud Computing nicht aus.

Die bedarfsgerechte Sicherheit virtualisierter Infrastrukturen erfordert ein koordiniertes Zusammenspiel von Netzwerk-, System-Management- und Security-Komponenten. Das beinhaltet unter anderem mehrere Verteidigungslinien, netztechnische Kapselung und Maßnahmen gegen eine unkontrollierte Verbreitung von Schadsoftware.Wichtig ist in jedem Fall eine ganzheitliche Sichtweise, die isolierte Betrachtung von Einzelkomponenten reicht nicht aus.

Am Ende steht eine individuelle Lösung, die alle nötigen Securitymaßnahmen umfasst. Das Unternehmen kann die Technologien nach Bedarf und modular von seinem Provider beziehen. Sollten spätere Risikoanalysen neue Dienste nötig machen, lassen sich die Maßnahmen jederzeit erweitern und anpassen.

Klare Trennung von Anwendungen und Daten

Trotz vieler Parallelen mit dem konventionellen Outsourcing stellt das Thema Sicherheit bei der Virtualisierung von Servern daneben einige besondere Anforderungen. Das betrifft vor allem den Datenschutz: Da sich im Rechenzentrum mehrere Unternehmen IT-Ressourcen von den gleichen Rechnern beziehen, muss zum Beispiel gewährleistet sein, dass niemand die Informationen des anderen sehen kann. Daten und Anwendungen der einzelnen Kunden müssen hierzu sauber voneinander getrennt sein. Das ermöglichen sogenannte virtuelle lokale Netzwerke (VLANs), das heißt, jedes Unternehmen erhält automatisch einen separaten Anschluss an den Server. Dieser verfügt somit je nach Zahl der Kunden über beliebig viele individuelle Zugänge.

Die Administration des VLANs erfolgt über eine zentrale Weiche. Alle Netzwerkkabel laufen hier zusammen. Die Weiche teilt jedes VLAN automatisiert einem bestimmten Kunden zu. Wen sie nicht kennt, lässt sie nicht auf diesen Zugang. Spionage- oder Manipulationsversuche bleiben somit erfolglos.

Nutzer bestimmt Standort der Wolke

Noch ein weiterer Punkt verhindert die Ausbreitung der Wolken und stellt einen großen Unterschied zum klassischen Outsourcing dar: Der Nutzer weiß in der Public Cloud à la Amazon nicht, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land der Provider seine Daten speichert. Das kann böse Folgen haben: Überschreiten die Daten Ländergrenzen, erfüllen sie unter Umständen Anforderungen an die datenschutzrechtliche und branchenspezifische Auflagen nicht mehr. Für die Wolke im Geschäftsumfeld eignen sich deshalb besonders Anbieter aus der Europäischen Union. Selbst in den USA existiert bislang kein mit der EU-Richtlinie 95/46/EG vergleichbarer Mindeststandard für den Datenschutz. Dort geht man mit Informationen deutlich freizügiger um. Beispielsweise kann jeder Bürger ohne Weiteres Behördenakten abrufen.

In der privaten Wolke von T-Systems bestimmt der Nutzer, in welchem Rechenzentrum seine Daten gespeichert sein sollen. Daneben besteht im Rahmen einer sogenannten Twin-Core-Strategie immer noch ein zweites Standbein: Alle Daten liegen in einem zweiten – ebenfalls Cloud-Computing-fähigen – Rechenzentrum gespiegelt vor. Die Synchronisation der Informationen findet während des laufenden Betriebs automatisch statt. Fällt am Hauptstandort ein Server aus oder kappt ein Bagger versehentlich eine Datenleitung, übernimmt der „Zwilling" über das Backup nahtlos die Funktion des ersten Data Centers. Das Geschäft des Kunden läuft damit jederzeit störungsfrei weiter.

Nutzt ein Unternehmen das Netz seines Dienstleisters, kann es mit diesem sogar Servicevereinbarungen für die Wolke vertraglich festlegen, die vom Rechenzentrum übers Netz bis zum PC oder mobilen Endgerät des Anwenders reichen. So lässt sich die Qualität und Verlässlichkeit der Dienste exakt kontrollieren und beurteilen. T-Systems kann im eigenen MPLS-Netz (Multi-Protocol Label Switching) Cloud-Anwendungen bei Bedarf sogar Vorfahrt gegenüber weniger kritischen Applikationen geben. So kommt es auch bei hohem Verkehrsaufkommen nicht zu Verzögerungen aufgrund von Datenstaus.

Fazit:

Mit Virtualisierung können Unternehmen Kosten senken, Abläufe verbessern und Ressourcen sparen. Nur wenige Firmen verfügen aber über das notwendige technische Know-how, geschweige denn über die personellen Ressourcen, um Cloud Computing mit der nötigen Sicherheit selbstständig zu realisieren. Dienstleister wie T-Systems arbeiten an vorderster technologischer Front um sichere Cloud-Infrastrukturen zu benchmarkfähigen Kosten zu gestalten und für jedes Unternehmen erschwinglich zu machen.

„Datenschutz ist kein lästiges Hemmnis“

Die TÜV Informationstechnik GmbH (TÜViT) steht als neutrale Institution dafür, den Datenschutz zu fördern und voranzubringen. Geschäftsführer Antonius Sommer warnt davor, den Aufwand für den Schutz von Informationen zu scheuen, denn davon kann der wirtschaftliche Erfolg der Unternehmen abhängen.

In welchen Bereichen führt TÜViT Datenschutz-Prüfungen durch?

Zunächst einmal ist Datenschutz ein zunehmend wichtiger werdendes Thema, nicht zuletzt dadurch, dass in jüngster Zeit etliche Skandale bekannt wurden. TÜViT bewertet IT-Produkte, IT-Systeme und IT-Prozesse auf ihren Datenschutz hin. Dies reicht von der Überprüfung einfacher Aktenvernichter bis hin zu umfangreichen Prozessketten wie dem komplexen Rechnungsprozess der Deutschen Telekom, bei dem sämtliche Verkehrsdaten der über 27 Millionen Telefonkunden verarbeitet werden. Hier wurde jetzt der erste Teil des Prozesses überprüft und erfolgreich zertifiziert. Mit dem Zertifikat bestätigen wir die Erfüllung aller Anforderungen an den Kundendatenschutz in diesem sensiblen Bereich.

Welche Mängel fallen am häufigsten auf?

Im Produktbereich sind beispielsweise Programme häufig noch nicht geeignet, den nötigen Datenschutz zu gewährleisten. Oder sie sind nicht konform mit den existierenden, vielfältigen Datenschutzbestimmungen und Richtlinien. Im Bereich der Verfahren, also automatisierten Vorgängen einer verarbeitenden Stelle, besteht die Gefahr, dass Daten nicht allein gemäß ihrer Zweckbestimmung verwendet werden oder der Zugriffsschutz ausschließlich durch Befugte nicht vollständig gewährleistet ist.

Welchen Nutzen sehen Sie in den Überprüfungen?

Im Bereich der Produkte erhalten Hersteller durch die Prüfung eine detaillierte, auf den Datenschutz ausgerichtete Dokumentation, die aus einem juristischen und einem technischen Teil besteht. Stellt sich heraus, dass ein Produkt nicht gesetzeskonform ist oder wenn in der Anwendung Schwachpunkte auftreten, kann das Produkt darauf hin überarbeitet und optimiert werden. Wird das Produkt aber zertifiziert, dann bedeutet dies einen - vielleicht entscheidenden - Wettbewerbsvorteil gegenüber den anderen Anbietern. Das Kundenvertrauen wird durch ein Zertifikat eines unabhängigen Dritten enorm gestärkt.

Und was haben Verfahrensbetreiber davon?

Verfahrensbetreiber können nachweisen, dass ihre Organisation sich freiwillig und proaktiv um den Datenschutz kümmert: Das sorgt für Transparenz nicht nur für die Kunden, sondern auch für Mitarbeiter und die Aufsichtsbehörden. Bezogen auf die Telekom können die Festnetzkunden nun sicher sein, dass ihre Daten vertraulich behandelt werden und keine unberechtigten Nutzer darauf zugreifen. Das ist ein wichtiges Signal, das natürlich das Vertrauen in das Unternehmen stärkt.

„Elektronische Kommunikation muss sicherer werden“

Holger Mühlbauer, Geschäftsführer des TeleTrusT Deutschland e.V., hat die Regierungsprogramme der deutschen Parteien vor der Bundestagswahl in Bezug auf ihre Aussagen zu IT-Sicherheit und Datenschutz analysiert. Ergebnis: FDP und Grüne machen sich mehr Gedanken.

Welchen Stellenwert hat die elektronische Kommunikation in Deutschland aus Ihrer Sicht mittlerweile erklommen?

Die E-Mail hat sich als Kommunikationsmedium ganz eindeutig durchgesetzt und ihre Bedeutung wird weiter wachsen. Damit wird auch ein weiter steigender Anteil von unternehmenskritischen Informationen elektronisch verschickt werden. Vor diesem Hintergrund muss ich auch darauf hinweisen, dass noch immer nicht alle Rechtsfragen geklärt sind.

Wann werden die denn geklärt sein?

Das ist schwer zu sagen. Der IT-Sicherheitsverband TeleTrusT Deutschland e.V. mit Sitz in Berlin wurde schon im Jahr 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. Dafür setzen wir uns nach wie vor vehement ein. Wir haben mit großer Spannung beobachtet, wie die Parteien sich vor der Bundestagswahl zu den Themen IT-Sicherheit und Datenschutz stellen und die Regierungsprogramme daraufhin analysiert. Das Ergebnis lässt daran zweifeln, dass alle Parteien die Bedeutung dieser Themen vollends begriffen haben.

Was haben Sie denn herausgefunden?

FDP und Grüne machen sich mehr Gedanken über IT-Sicherheit und Datenschutz als andere Parteien. Die Aussagen weisen zudem in Teilen eine recht hohe Detailschärfe auf. Allerdings werden Schlagworte der aktuellen politischen Diskussion wie die ‚elektronische Signatur‘, ‚De-Mail‘ und ‚Authentifizierung‘ nirgendwo ernsthaft aufgegriffen – bestenfalls werden sie indirekt behandelt. Auch die Bürgerkarte kommt praktisch nicht vor.

Was raten Sie Unternehmen? Wie kann eine sichere elektronische Kommunikation gewährleistet werden?

Sicher ist, dass die E-Mail-Verschlüsselung an Bedeutung gewinnen muss, um

sensible Inhalte zu schützen und um eine rechtssichere Kommunikation zu gewährleisten. Die Art der gewählten Technologie hängt von den Inhalten, den organisatorischen Umständen und der Handhabbarkeit ab. Unternehmen müssen sicherstellen, dass sie ihre Kommunikationssysteme technisch und rechtssicher beherrschen. Dazu ist eine permanente Analyse der Anforderungen und Gefährdungssituationen notwendig, wobei nicht nur Angriffe von außen und innen, sondern auch technisches und menschliches Versagen in Betracht kommt. Die elektronische Kommunikation muss auf jeden Fall sicherer werden.

„Investitionen in IT-Sicherheit richtig bewerten“

IT-Sicherheit sollte nicht als zentraler Kostenblock geführt und im Gießkannenprinzip im Unternehmen umgelegt werden, fordert Prof. Dieter Kempf, Präsidiumsmitglied des BITKOM und Vorstandsvorsitzender von Deutschland-sicher-im-Netz.

Herr Prof. Kempf, die Bedeutung von IT hat in Unternehmen fast aller Branchen stark zugenommen. Doch noch immer müssen einige Anwender überzeugt werden, in ihre IT-Sicherheit zu investieren. Warum?

Die Vorteile einer neuen IT-Anwendung für den Geschäftsbetrieb sind den Unternehmen in der Regel klar. Denn die funktionalen Anforderungen sind detailliert beschrieben und es liegt eine entsprechende Wirtschaftlichkeitsbetrachtung vor. Bei der IT-Sicherheit erleben wir hingegen häufig große Zweifel. Es kommen Fragen wie: „Was muss ich als Unternehmen eigentlich beim Thema IT-Sicherheit tun? Wie viel muss ich wofür investieren? Bisher ist uns doch nichts passiert – lohnt sich das Ganze überhaupt?“ Das führt leider häufig dazu, dass die Verantwortlichen am Ende andere Prioritäten setzen.

Spielt die Investitionszurückhaltung in der aktuellen Wirtschaftskrise auch eine Rolle?

Der Rechtfertigungsdruck für Sicherheitsinvestitionen ist gerade in Krisenzeiten extrem hoch. In den Unternehmen ist der Investitionsrahmen in der Regel gedeckelt. Vereinfacht gesagt: Investitionen konkurrieren intern miteinander – und was einen niedrigen oder negativen Return of Investment hat, wird häufig nicht umgesetzt. IT-Sicherheit liefert in den meisten Fällen keinen eigenen, separat ausweisbaren Wertbeitrag. Deshalb müssen wir noch stärker eine Diskussion um den Return of Security Invest (ROSI) führen.

Wie können Unternehmen mit diesem Dilemma umgehen?

IT-Sicherheit sollte nicht als zentraler Kostenblock geführt und im Gießkannenprinzip im Unternehmen umgelegt werden. Unternehmen müssen vielmehr die realen Wechselwirkungen zwischen Geschäftsbetrieb – also dem jeweiligen Geschäftsprozess – und der IT-Sicherheit für die Entscheider transparent machen.

Auf welche Weise kann das geschehen?

Zumindest für die zentralen und existenziellen Geschäftsprozesse sollten die Konsequenzen von Ausfällen und Störungen bekannt sein. Was passiert beispielsweise, wenn der Server eines Online-Shops nicht zur Verfügung steht oder die Kundendatenbank gehackt wird? Oft geht es dabei um Sein oder Nicht-Sein. Hieraus lassen sich verbindliche Sicherheitsziele ableiten, für die dann Maßnahmen getroffen werden müssen. Darüber sollte es dann keine Diskussion mehr geben. Am Ende muss diejenige Maßnahme ausgewählt werden, die die Sicherheitsziele erfüllt und die sich der betroffene Geschäftsprozess aufgrund seines Wertbeitrages leisten kann. Die Banken haben das inzwischen verstanden: Ein überzeugendes IT-Sicherheitskonzept ist häufig ein positives Kriterium bei der Kreditwürdigkeitsprüfung.

„Schutz von Informationen wird das Thema der Zukunft sein“

Frank Fischer, Leiter Sicherheitslösungen bei IBM, plädiert für ein Umdenken beim Thema Internetsicherheit. Nicht mehr nur die technischen Lösungen zum Abwehren von Angriffen sollten im Vordergrund stehen, sondern Strategien zur Handhabung sensibler Informationen. Doch dafür muss oft erst einmal das Bewusstsein geschaffen werden.

IT-Sicherheitslösungen werden immer ausgefeilter, aber auch die Angriffe aus dem Web. Wie stellt sich ihrer Meinung nach die aktuelle Bedrohungssituation dar?

Die Bedrohungslage ist nach wie vor kritisch. Nur macht uns nicht mehr nur die schiere Masse der Angriffe zu schaffen, sondern vor allem deren zunehmende Qualität. Und damit meine ich vor allem die intelligente Verknüpfung von geringem Aufwand mit höchstmöglicher Schadenswirkung. Diese erreichen Schadprogramme mittlerweile nicht mehr nur mit dem Angriff auf komplexe Softwarepakete, sondern vermehrt mit der Manipulation einfacher, aber weit verbreiteter und oft genutzter Anwendungen wie Editoren oder Flash-Applikationen. Viele dieser Programme stammen von kleineren Herstellern, die oftmals nicht die Ressourcen haben, um Schwachstellen rechtzeitig zu schließen. Das ist natürlich eine ideale Situation für Hacker.

Was sollte ihrer Meinung nach eine umfassende Internet-Security-Lösung leisten?

Die Grundvoraussetzung für ein erfolgreiches Sicherheitskonzept ist die richtige Einschätzung der Bedrohungslage. Dazu gehört auch, sich zunächst Gedanken darüber zu machen, welche Informationen unbedingt schützenswert sind, also was das Interesse eines Angreifers sein könnte. Erst dann ist es sinnvoll, über Maßnahmen zum klassischen Perimeterschutz nachzudenken, also das Filtern unerwünschter Anfragen und Abwehren von Angriffen auch technisch umzusetzen. Unabhängig von einzelnen Ansätzen geht es grundsätzlich darum, das Thema Sicherheit von einem reinen Technik-Image zu lösen, das ja für viele immer noch geprägt ist vom Bild eher lästiger Schutzmaßnahmen wie zum Beispiel vermehrte Passwortabfragen. Für den Erfolg im Unternehmen ist es ganz entscheidend, dass ein IT-Sicherheitskonzept nicht nur einen Versicherungscharakter hat, sondern auch als werthaltig wahrgenommen wird.

Die Bedrohungslage im Internet zeichnet sich durch eine hohe Dynamik aus. Welche Trends sind für die Zukunft zu erwarten?

Das Thema der Zukunft wird der Informationsschutz sein. Und zwar nicht nur im technischen Sinne, sondern vor allem im Hinblick auf ein Umdenken in der Handhabung von Information. Schon heute ist ein erstaunlich großer Teil aller Angriffe nicht auf einen Vorsatz, sondern auf die Fahrlässigkeit der Nutzer zurückzuführen. Für die Zukunft wird es deshalb immer wichtiger, Menschen im Umgang mit Informationen zu schulen, und zwar am besten schon im Jugendalter. Wir bei IBM sehen das durchaus auch als soziale Verantwortung.

„Angriffe von Cyberkriminellen werden immer intelligenter“

Interview mit Lothar Symanofsky, Gesamtleitung Vertrieb und Marketing BitDefender GmbH

Wo sieht BitDefender derzeit die größten Defizite beim Mittelstand hinsichtlich IT-Sicherheit?

Viele Unternehmen gehen allzu sorglos mit ihrer IT-Sicherheit um, was auch die jüngsten Umfrageergebnisse bestätigen. Doch selbst dann, wenn die IT-Sicherheit als Top-Thema von den Inhabern und Geschäftsführern betrachtet wird, scheitern diese bei der Umsetzung eines unternehmensweiten Sicherheitskonzepts für ihre Firmen. Dies ist auf fehlende personelle Ressourcen, den Mangel an hochkarätigen IT-Sicherheitsexperten und limitierten Budgets zurückzuführen. Deshalb benötigen sie einen erfahrenen Partner, der über das notwendige Experten-Know-how, die erforderliche Sicherheitssoftware sowie Beratungspartner (die sich direkt vor Ort befinden) verfügt und einen umfangreichen Support-Service aus einer Hand offerieren kann. Das alles zu Konditionen, die dem Mittelstand ein attraktives Preis-Leistungs-Verhältnis bieten.

Auf welche zukünftigen Gefahren müssen sich die Unternehmen einstellen?

Neben der zunehmenden Komplexität der Internet-Attacken wird auch deren Zahl drastisch zunehmen. Damit wird die Netzwerksicherheit einen zentralen Punkt einnehmen. Botnetze werden sich weiterentwickeln und nur noch schwer aufzuspüren sein. SPAM- und Phishing-Angriffe werden zunehmend intelligenter programmiert. Wichtigstes Mittel dagegen sind heuristische Techniken wie BitDefender B-HAVE, die Bedrohungen mit neuen und unbekannten Signaturen aufspüren und neutralisieren. Produkte aus dem Hause BitDefender bieten bereits heute Erkennungsraten, die weit über denen vergleichbarer Produkte liegen. Um auch auf zukünftige Bedrohungen optimal reagieren zu können, wird in unseren rumänischen Entwicklungslaboren permanent an neuen Technologien für den Kampf gegen Malware geforscht.

Welche Auswirkungen hat die Wirtschaftskrise auf die IT-Sicherheit?

In Zeiten wirtschaftlicher Turbulenzen bleibt der finanzielle Aspekt beim Schutz vor Cyberkriminalität nicht außen vor. Eine Security-Suite soll nicht nur effektiv sein, sie soll gleichzeitig die Kosten für die Netzwerkverwaltung möglichst gering halten. Hier sind Unternehmen deutlich preissensitiver geworden und fordern einen größtmöglichen Schutz bei geringst möglichem Total Cost of Ownership. Außerdem ermöglicht ein zentrales Management-System, das in guten Security-Suiten heutzutage enthalten sein muss, durch verringerte Administrationskosten einen hohen Return-on-Investment. Durch den Einsatz einer Security Suite, wie beispielsweise der BitDefender Client Security, werden die Kosten für das Sicherheitsmanagement und die Beseitigung von Malware-Schäden für Unternehmen effizient gesenkt. Die Sicherheitslösungen von BitDefender bieten neben der zentralen Administration außerdem eine automatische Kontrolle des gesamten Unternehmensnetzwerkes.

„Keine Angst vor der Cloud“

Kommentar von Olaf Heyden, Geschäftsführer T-Systems und Leiter ICT Operations

In der Sache sind sich Analysten und IT-Chefs einig: Cloud Computing ist eine Option, IT-Kosten zu senken. Doch ist die Wolke sicher?

Laut Ergebnissen einer aktuellen Studie des US-amerikanischen Marktforschungsunternehmens Applied Research verlässt Cloud Computing gerade seinen Hype-Status und peilt die kritische Masse an. Mehr als 80 Prozent von 250 befragten IT-Managern großer Unternehmen in den USA gaben an, zumindest versuchsweise Cloud-Computing-Projekte gestartet zu haben.

Doch je mehr Cloud Computing ins Rampenlicht tritt, desto lautstärker melden sich Bedenkenträger: Aus Sicherheitsgründen sei die Zeit für IT-Dienstleistungen aus der Wolke noch nicht reif. Viele Argumente der Skeptiker erinnern dabei an die Gegner des Outsourcings, die geschäftskritische Informationen keinem Dritten anvertrauen wollen und Angst vor Netzausfällen und Datenverlust hatten.

Dabei darf man allerdings nicht öffentliche Clouds à la Google mit privaten Clouds für Unternehmen gleichsetzen. Privatnutzer der Google-Welt mieten Speicherplatz für E-Mails und Urlaubsfotos auf einem Server irgendwo in der Welt – dies umsonst und ohne Verpflichtungen und Servicevereinbarungen des Anbieters.

Wer sich dagegen als Unternehmen für Cloud Computing entscheidet, weiß, wie viele Rechenzentren der Dienstleister besitzt und wo sie stehen. Er kann vertraglich festlegen, welche Anwendungen in welchen Rechenzentren und welche seiner Daten in welchem Land gespeichert sind. Damit sind auch die gesetzlichen Compliance-Anforderungen erfüllbar. Kein Vergleich also mit dem Cloud Computing im öffentlichen Netz.

Für die Wolke im geschäftlichen Umfeld eignen sich besonders Anbieter aus der Europäischen Union. Mit der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr hat die EU einen Mindeststandard für den Datenschutz und die Datensicherheit eingeführt. So setzt zum Beispiel jede Übermittlung personenbezogener Informationen die vorherige Einwilligung des Betroffenen voraus. Auftragsdaten dürfen nur in den Grenzen der EU beziehungsweise des Europäischen Wirtschaftsraums (EWR) verarbeitet werden.

In den modernen Rechenzentren der spezialisierten ICT-Dienstleister wie T-Systems hat Sicherheitsmanagement jedenfalls oberste Priorität, denn auch für das klassische Outsourcing gelten die gleichen hohen Anforderungen wie für das Cloud Computing. Diese Sicher-

heitsvorkehrungen sind derart streng und umfangreich, dass sie nur von einem Spezialisten effizient umgesetzt werden können. Wer Sicherheit auf höchstem Niveau dagegen nur für sich selbst erreichen will, ist mit Kosten konfrontiert, die einen der größten Budgetposten des ICT-Betriebs ausmachen kann.

Die drei Datenschutznovellen 2009

Der Gesetzgeber hat das Bundesdatenschutzgesetz (BDSG) 2009 einer dreimaligen Novellierung unterzogen, die größtenteils im September 2009 in Kraft tritt – mit weitreichenden Konsequenzen für die Unternehmen.

VON RA KARSTEN U. BARTELS LL.M. , Regionalbeauftragter der Arbeitsgemeinschaft Informationstechnologie (davit) im Deutschen Anwaltverein für Berlin-Brandenburg

Neu sind Vorschriften zur Datenübermittlung an Auskunfteien und zum Scoring, §§ 28a f. BDSG. Erlaubnistatbestände und Verfahrensvorschriften regeln nun die Erhebung und Verarbeitung von Daten über die wirtschaftliche Lage des Betroffenen sowie Prognosen über ein zukünftiges Verhalten. Festgelegt ist z. B., wann eine Forderung übermittelt werden darf, und welche Maßgaben für die Verfahren zur Wahrscheinlichkeitsberechnung gelten. Betroffene sind nicht nur Kreditnehmer, sondern auch zunehmend Käufer im Versandhandel und Mieter von Immobilien. Nahezu unbemerkt sind zudem Pflichten für entsprechende Datenbankbetreiber im Zusammenhang mit Auskunftsverlangen aus EU-Mitgliedsstaaten bzw. Staaten des EWR eingeführt worden.

Gestärkt wurde die Stellung des betrieblichen Datenschutzbeauftragten durch Erweiterung des Kündigungsschutzes während und innerhalb eines Jahres nach Beendigung seiner Bestellung, § 4f Abs. 3 BDSG.

Der zulässige Adresshandel wurde eingeschränkt (sog. Listenprivileg), § 28 Abs. 3 BDSG. Es ist nun grundsätzlich eine qualifizierte Einwilligung des Betroffenen in die Verarbeitung oder Nutzung erforderlich (opt-in). Empfänger von Werbeschreiben müssen über die ursprüngliche Herkunft der Daten informiert werden. Ein relatives Kopplungsverbot verbietet, dass ein Vertragsschluss von dieser Einwilligung abhängig gemacht wird, allerdings nur, soweit es sich um Unternehmen mit marktbeherrschender Stellung handelt.

Bei der Auftragsdatenverarbeitung muss der Auftragsinhalt künftig wesentlich umfassender schriftlich fixiert werden, § 11 BDSG. Neuregelungen gibt es auch für den Bereich der Markt- und Meinungsforschung, § 30a BDSG.

Ein spezifischer wie rudimentärer Arbeitnehmer-Datenschutz sieht nun vor, dass personenbezogene Daten im Rahmen eines Beschäftigungsverhältnisses lediglich verarbeitet werden dürfen, wenn dies für die Begründung, die Durchführung oder die Beendigung des Beschäftigungsverhältnisses erforderlich ist, § 3 Abs. 11 BDSG. Es wird klargestellt, dass datenschutzrechtlich relevante Maßnahmen zur Aufdeckung von Straftaten eines Arbeitnehmers nur durchgeführt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte für eine Straftat vorliegen, § 32 Abs. 1 BDSG.

Bei schwerwiegenden Datenschutz-Pannen trifft die Verantwortlichen nun eine umfangreiche Informationspflicht, die von einem strafrechtlichen Verwertungsverbot flankiert wird, § 42a BDSG. Die zuständigen Datenschutzaufsichtsbehörden sowie die Betroffenen sind unverzüglich zu informieren. Unverzüglich ist die Information der Betroffenen auch dann noch, wenn ggf. zunächst Maßnahmen zur Sicherung der Daten zu ergreifen sind und eine Gefährdung der Strafverfolgung nicht mehr zu befürchten ist (sog. responsible disclosure).

Die Bußgeldtatbestände und der Bußgeldrahmen wurden erheblich ausgeweitet bzw. erhöht und können je nach Verstoß eine Höhe von bis 50.000 bzw. bis zu 300.000 EUR erreichen, § 43 BDSG. Da das Bußgeld nicht nur den Vorteil aus der Ordnungswidrigkeit abschöpfen, sondern übersteigen soll, können die Bußgelder die genannten Rahmen auch empfindlich übersteigen. Die Aufsichtsbehörden wurden zudem mit der Befugnis ausgestattet, Maßnahmen zur Beseitigung von Datenschutzverstößen anzuordnen, § 38 Abs. 5 BDSG.

Das umstrittene Datenschutzaudit-gesetz ist letztlich nicht verabschiedet worden. Stattdessen wurde ein dreijähriges Modellprojekt in einer noch zu bezeichnenden Branche beschlossen.

Die TOP 10 Tabus im Datenschutz

1. Datenschutz ist nicht Chefsache
2. Kein (qualifizierter) betrieblicher Datenschutzbeauftragter
3. Fehlendes/fehlerhaftes Verfahrensverzeichnis
4. Fehlende Verpflichtung der Mitarbeiter auf den Datenschutz
5. Fehlerhaftes Outsourcing
6. Produktentwicklung ohne Einbeziehung des Datenschutzrechts
7. Data Mining, Data Warehouse
8. Direkt Marketing ohne erforderliche Einwilligungen
9. Außerachtlassung möglicher Haftungsszenarien
10. Websites: Unzulässige Datenerhebung; fehlende/fehlerhafte Datenschutzerklärung

„Es werden neue, innovative Sicherheitslösungen kommen“

Prof. Dr. Norbert Pohlmann, Vorstandsvorsitzender des TeleTrusT Deutschland e.V.

Professor Norbert Pohlmann ist Experte für Trusted Computing und Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen. Er glaubt, dass elektronische Geschäftsprozesse mit einer Sicherheitsplattform auf der Basis von TPM-Technologie in Zukunft deutlich sicherer gemacht werden wird.

Glauben Sie, dass es Sicherheitslösungen geben kann, die verlässlich vor jeder Art von Malware – also auch vor Trojanern – schützen kann?

Eine 100-prozentige Sicherheit wird es wohl nie geben, aber im Moment liegen wir im Kampf gegen die Schadprogramme viel zu weit zurück. Das darf so nicht bleiben und das wird so nicht bleiben! Es werden neue, innovative Sicherheitslösungen kommen, mit denen die Internet-Kriminellen auf fremden Rechnern kaum noch Chancen haben werden.

Wie könnten solche Sicherheitslösungen denn aussehen?

Wir in Gelsenkirchen arbeiten an Sicherheitsmethoden, mit denen Software gemessen und damit kontrolliert wird. Es werden bestimmte Sicherheitsbereiche auf dem Rechner eingerichtet, in denen nur absolut vertraute Software ablaufen darf. In diesen so genannten Compartments ist die saubere Software, die für sicherheitskritische Anwendungen benötigt wird, so zu sagen stark isoliert, das heißt gegen Angriffe geschützt. Diese Sicherheitsbereiche können nicht infiziert werden. Jeder unbekannte Code, also jede Malware, wird ausgeschlossen.

Ist das Zukunftsmusik oder eine Lösung, die in absehbarer Zeit eingeführt werden kann?

Eine relativ zügige Einführung solcher Sicherheitslösungen in den Markt halte ich für sehr gut denkbar und notwendig. Entscheidend ist, dass die Hardware solche Sicherheitslösungen unterstützt. Das ist aber schon weitgehend der Fall. Heute ist schon fast jedes Notebook mit einem TPM-Chip ausgestattet. Die Firmen müssen jetzt konsequent beginnen, solche Sicherheitsplattformen auf der Basis der TPM-Technologie einzuführen, was wahrscheinlich bedeuten wird, dass einige wenige Rechner ausgetauscht werden müssen, die noch keine TPMs unterstützen. Es muss uns völlig klar sein, dass wir einen solchen Quantensprung in der IT-Sicherheit schnell brauchen, um weitere Potentiale der elektronischen Geschäftsprozesse vertrauenswürdig nutzen zu können.

Sicherheit in der Wolke

Die Verlagerung der Rechenumgebung vom Desktop ins Internet lässt Sicherheitsbedenken aufkommen. Kann man darauf vertrauen, dass die eigenen Daten auf den Servern einer anderen Firma in der so genannten „Cloud“ sicher sind?

VON KAI GUTZEIT, Head of Google Enterprise DACH & Nordics

Beim Cloud Computing werden IT-Software und -Services über das Internet und einen Browser bereitgestellt. Dies ist ein Paradigmenwechsel – so als würden Sie Ihren Goldschmuck in der Sockenschublade aufbewahren und dann irgendwann zur Bank bringen. Die Bank hat die Skaleneffekte. Sie investiert mehr in Sicherheit als Sie je zu investieren in der Lage wären. Das gilt auch für Daten. Große Cloud-Computing-Anbieter verfügen über die nötige Ausstattung, um Millionen von Nutzerdaten zu schützen.

Sicherheit ist eine immense Herausforderung für Unternehmen. Laut einem Bericht von Credant Technologies haben Londoner Taxifahrgäste im Jahr 2008 innerhalb von sechs Monaten über 60.000 Handheld-Geräte auf den Rücksitzen der „Black Cabs“ vergessen.

Unternehmen verwenden viel Zeit und Ressourcen auf den Datenschutz. Was also geht schief? Drei Viertel aller Fälle von Datenverlust basieren auf menschlichem Versagen. Dabei haben Mitarbeiter keine bösen Absichten. Sie möchten zu Hause arbeiten, um ihr Pensum zu schaffen. Ermöglichen Sie ihnen den orts- und zeitunabhängigen Zugriff auf Daten. Die sind immer sicher in der Cloud gespeichert, und Sie vermeiden automatisch Datenverlust-Risiken.

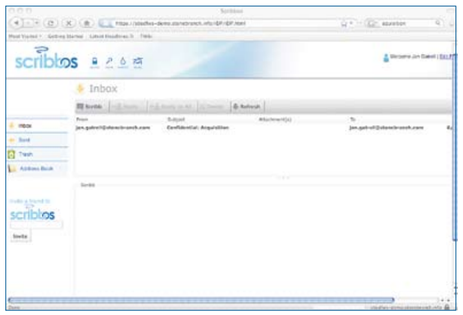
Die Cloud bietet weitere Sicherheitsvorteile. Unternehmen benötigen meist 30 bis 60 Tage, manche drei bis sechs Monate, um Sicherheitspatches auf ihren Systemen zu installieren. Wir betreiben hingegen eine homogene Rechenumgebung. Wenn ein Patch vorliegt, kann er schnell und einheitlich auf allen Systemen implementiert werden.

Auch die physische Sicherheit der Rechenzentren und die Zuverlässigkeit unserer Cloud-Computing-Angebote sind gewährleistet. Bei uns werden die Nutzerdaten zu verschiedenen Rechenzentren repliziert. Wenn ein Rechenzentrum ausfällt, hilft unsere Infrastruktur, die Datensicherheit und den Zugriff auf die Daten sicherzustellen.

Nun ist kein System hundertprozentig ausfallfrei oder komplett sicher. Jedes System wird irgendwann von Sicherheitsproblemen betroffen sein. Die entscheidende Frage ist: Über welches Personal, welche Prozesse und welche Technologien verfügen Sie, um die Auswirkungen dieser Störfälle auf ein Minimum zu beschränken, und wie schnell können Sie auf Probleme reagieren? Bei uns ist ein Team rund um die Uhr verfügbar, das auf Bedrohungen schnell reagiert. Mehr als 1,75 Millionen Unternehmen, die unsere Cloud-Computing-Angebote nutzen, sind davon überzeugt, dass diese Cloud-basierten Lösungen kosteneffizient, kollaborativ und sicherer sind.

Das wachsende Rauschen in der Unternehmenskommunikation

Zunehmender Daten- und Informationsaustausch stellt Unternehmen vor immer größere Probleme



In der modernen Welt spielt Kommunikation eine immer größere Rolle. Gleichzeitig nimmt die Zahl der Kommunikationsformen stetig zu: Heutzutage nutzt jeder E-Mail, SMS, Telefon, Fax, soziale Netzwerke, aber auch Protokolle wie FTP zur Übertragung großer Dateien. Vor allem im Geschäftsumfeld führt dies jedoch zunehmend zu Problemen mit der Sicherheit. Dazu reicht ein Blick in die Nachrichten: Dort stößt man immer wieder auf Datenlecks, Verluste von persönlichen Informationen oder die Möglichkeit, sensible Daten über das Internet zu erstehen,

Für die IT bedeutet dies, dass die bestehenden Kommunikationskanäle keinen ausreichenden Schutz bieten, insbesondere bei geschäftskritischen Daten und Inhalten. Täglich schicken Angestellte und Manager solche Informationen per E-Mail an Kunden und Geschäftspartner. Die Ausmaße der E-Mail-Kommunikation lassen sich durch eine Zahl des Analystenhauses Gartner verdeutlichen: Alle vier Wochen werden über E-Mail-Systeme acht Terabyte Daten übertragen. Das Problem dabei ist, dass sich eine E-Mail im Prinzip wie eine Postkarte lesen lässt. Auch die in fast jedem Unternehmen verbreitete Nutzung von FTP zur Übertragung großer Dateien ist alles andere als sicher.

Um zu garantieren, dass bei der täglichen internen und externen Kommunikation keine Sicherheitslücken entstehen und sensible Informationen entsprechend geschützt werden, bedarf es einer absolut zuverlässigen Lösung. Mit Scribbos bietet der Managed File Transfer- und Job Scheduling-Spezialist Stonebranch die erste unternehmenstaugliche Lösung in diesem Bereich an. Das Produkt ist in verschiedenen Versionen erhältlich: als Software-as-a-Service-Angebot (SaaS) oder zur Installation auf einem eigenen Unternehmensserver.

Die Anwendungsmöglichkeiten von Scribbos sind dabei beinahe unbegrenzt: Einzelpersonen wie Rechtsanwälte, Ärzte oder Architekten können sensible Daten ebenso einfach und sicher versenden wie große Unternehmen. Diese haben die Möglichkeit, Scribbos zum Versand von geschäftskritischen Informationen in der anfallenden Ad-Hoc-Kommunikation und bei der Übertragung großer Dateien zu nutzen. Vor allem durch die Einbindung von Infitran, der Managed File Transfer Lösung von Stonebranch, lässt sich Scribbos von zentraler Stelle aus managen und überwachen. Unternehmen können so den stetig steigenden Compliance-Anforderungen gerecht werden.

Und Scribbos ist denkbar einfach zu bedienen: Wer eine E-Mail versenden kann, kann auch Scribbos nutzen.

Mehr Informationen zum sicheren Datenaustausch finden Sie unter: **www.scribbos.com**

Ein Weg aus dem Passwortdilemma?

Von domänen-basierten zu offenen Identitätsmanagementmodellen

VON IVONNE THOMAS, MICHAEL MENZEL

Die Registrierung und Verwaltung von Benutzeraccounts, so genannten digitalen Identitäten, bei verschiedenen Dienstleistern im Internet (Online-Shopping, Emailanbietern, etc.) ist für die meisten Internetnutzer mühsam und aufwendig. Nichtsdestotrotz benötigen viele Internetanbieter Information über ihre Nutzer. Der dabei vorherrschende so genannte anwendungs- oder dienstspezifische Ansatz Identitäten zu verwalten, führt zunehmend zu Problemen bei der sicheren Verwaltbarkeit von Zugangsdaten.

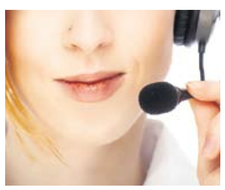
Die Lösung sind neue, offene Identitätsmanagementansätze, wie das föderative und das benutzerzentrische Identitätsmanagement, welche speziell für die dezentrale heterogene Landschaft des Internets geschaffen wurden. Offene IDM-Modelle basieren auf der Idee digitale Identitäten durch mehrere Systeme zu verwalten und gemeinsam zwischen zwei oder mehreren administrativ eigenständigen Teilnehmern auszutauschen. Die grundlegende Voraussetzung dabei ist die Existenz einer Vertrauensbeziehung zwischen dem Anbieter von Informationen (= Identity Provider) und dem, der die Information benötigt (die so genannte Relying Party). Bestimmte Aufgaben des Identitätsmanagements wie die Authentifizierung von Benutzern wird von der Instanz übernommen, bei der der Benutzer seine digitale Identität registriert hat.

Sowohl das benutzerzentrische als auch das föderative Identitätsmanagement funktionieren auf der Basis dieses Prinzips. Der entscheidende Unterschied ist die Art und Weise wie das für den Austausch notwendige Vertrauen etabliert wird. Beim föderativen Identitätsmanagement geschieht dies, indem sich die Teilnehmer zu einem Vertrauenszirkel, einer so genannten Föderation, zusammenfinden. Verträge schaffen dabei das notwendige Vertrauen. Föderatives Identitätsmanagement ermöglicht Single-Sign-On über mehrere Unternehmen. Um SSO Funktionen zu nutzen, hat der Benutzer die Möglichkeit seine Accounts in verschiedenen Unternehmen zu verbinden. Einmal authentifiziert kann er auf alle verlinkten Accounts zugreifen, unabhängig davon, ob er diese im eigenen Unternehmen oder in einem Partnerunternehmen hat. Beim benutzerzentrischen Modell bestehen im Allgemeinen keine vertraglichen Beziehungen zwischen zwei Partnern. Stattdessen entscheidet die abhängige Partei, welchen Partnern sie vertrauen möchte. Benutzerzentrisches Identitätsmanagement funktioniert damit sehr ähnlich wie die Verwaltung von Identitäten in der realen Welt. Verschiedene Behörden oder verwaltende Stellen geben Ausweise aus (sei es der Führerschein, Mitarbeiterausweis oder die Kundenkarte), mit denen der Benutzer bestimmte Aussagen über sich beweisen kann. Ein Dienstanbieter der realen Welt, wie beispielsweise ein Kinobetreiber, kann diesen vertrauen oder nicht. Mit OpenID und InformationCard existieren heute zwei Technologien, die den benutzerzentrischen Ansatz auch in der digitalen Welt umsetzen, wobei OpenID ein für das Web entwickeltes Protokoll darstellt während InformationCard auf den Web Service Technologien aufbaut.

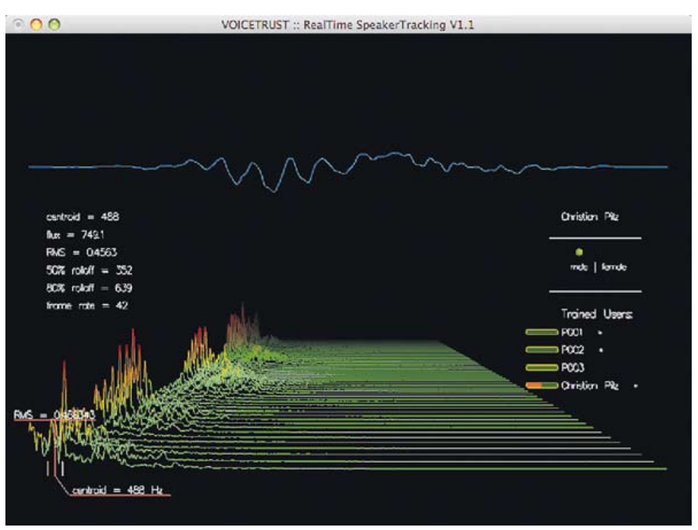
Die ersten Grundlagen für eine effizientere Verwaltung von digitalen Identitäten im Internet sind also geschaffen und Benutzer können hoffen, dem Passwortdilemma im Internet eines Tages Einhalt zu gebieten. Wie bei allen neuen Technologien, bleibt jedoch auch hier abzuwarten, inwieweit sich die neuen Ansätze in der Zukunft behaupten können.

Moderne Stimmbiometrie à la „Sesam öffne Dich“

Ein Sicherheits-Plus, das Geld spart, keine neue Hardware erfordert und den Nutzerkomfort steigert



VON RICHARD TIGGES



„Meine Stimme ist mein Passwort“ spricht ein Passant in sein Handy. Kurz darauf lächelt er: Der Bank-Computer hat ihn an seinem Erkennungssatz als Kunden identifiziert. Das Schöne an modernster Stimmbiometrie: sie funktioniert ortsunabhängig und ist nicht zu fälschen, auch nicht durch Stimmimitatoren. Biometrieverfahren greifen auf einzigartige Erkennungsmerkmale zurück, die dem menschlichen Körper eigen sind. Dazu muss keine neue Hardware gekauft werden. Ein Telefon hat jeder bei sich, einen Iris-Scanner oder Fingerabdruck-Leser wohl weniger. Durch die beschleunigte Identitätsüberprüfung und ihre völlige Automatisierbarkeit trägt Stimmbiometrie sogar zur Kostensenkung bei.

Sprecher-Erkennung ist nicht zu verwechseln mit Sprach-Erkennung. Es geht es darum, wer spricht, nicht was er spricht. In den USA hat sich Trade Harbour auf das Signieren von Dokumenten per Stimme spezialisiert und VoiceVerified hat einige Callcenter als Kunden. In Kanada beliefert Diaphonics Sound Security vor allem Regierungen mit Stimmerkennungslösungen für Sicherheitszwecke im Hochsicherheitsbereich. Es gibt sogar Sprecher-Erkennung auf dem Markt, bei der der Betroffene überhaupt nichts davon weiß, etwa in der Telefonüberwachung – Geheimdienste sollen bereits mit dieser Technologie arbeiten.

Auf textunabhängige Stimmerkennung verzichten hiesige Anbieter klassischer Unternehmens-Anwendungen bewusst, schon allein wegen des Betriebsrats und der in Deutschland strengen Datenschutzregeln. Zum Beispiel beim Password Reset Verfahren per Stimme, das der deutsche Anbieter Voicetrust zum Industriestandard gemacht hat. Damit können gesperrte Nutzerkonten in Firmennetzwerken per automatisiertem Telefondialog frei geschaltet werden, sobald der Anwender an der Stimme erkannt wurde. 1,8 Millionen Menschen haben dafür bereits ihr Stimmprofil hinterlegt. Sie können sich später eindeutig zu erkennen geben und peinliche Situationen schnell meistern: Passwort vergessen, PIN der EC-Karte verlegt, PUK zum Entsperren des Handys verloren.

Auch IBM engagiert sich auf diesem Sektor. Denn für Callcenter, Banken, Versicherungen, Mobilfunkanbieter und auch Mittelständler bedeutet Stimmbiometrie ein großes Sicherheitsplus. Früher konnte niemand garantieren, dass der Anrufer mit Kundenpasswort auch wirklich der rechtmäßige Besitzer eines Nutzerkontos war. Erst die Stimm-Authentifizierung gibt Anmeldeverfahren im IT-Bereich heute das nötige Quäntchen Sicherheit. Es gibt jetzt sogar einen mobilen Geheimnisspeicher für Endkunden, der nur per Stimme zu öffnen ist. Der „Voicesafe“ ist als Ansagedienst für Mobiltelefone oder als Stand-Alone Applikation fürs iPhone zu haben.

Fachmesse it-sa

Drei Tage IT-Sicherheit in Nürnberg

Vom 13.-15. Oktober findet nach ihrem Umzug von München die IT-Security-Messe it-sa erstmals in Nürnberg statt.

Die it-sa hat sich als die „Sicherheitshalle" auf der ehemaligen Systems etabliert und gehört schon seit zehn Jahren neben der Infosecurity in London und der RSA Conference in San Francisco zu den weltweit bedeutendsten IT-Security Events. Dabei versteht sich die it-sa als „Marktplatz" im ursprünglichen Sinne. Hier treffen sich Eperten und all jene, die beruflich etwas mit IT-Sicherheit zu tun haben, um Produkte live zu erleben, Informationen auszutauschen und Neuigkeiten zu erfahren. Damit ist die Messe auch am neuen Standort in Nürnberg die ideale Networking-Plattform für Führungskräfte und IT-Security-Spezialisten.

Konzentration auf IT-Sicherheit

Die mehr als 250 Aussteller, die aus Systems-Zeiten bekannten Foren sowie ein umfangreiches Kongressprogramm ermöglichen eine in der IT-Messelandschaft einmalige Konzentration auf das Thema IT-Sicherheit. Besucher der Messe erwartet eine große Bandbreite an Produkten und IT-Security-Lösungen, die es in dieser konzentrierten Form nirgendwo sonst gibt. Ob zum Thema Mobile Security, Physische Sicherheit, Datenrettung oder auch elektronischer Personalausweis – auf der it-sa findet man den richtigen Ansprechpartner. Selbst spezialisierte Branchenlösungen, z.B. für Banken, Kliniken, Steuerberater oder Rechtsanwälte werden geboten.

Ergänzend zur Messe gibt es für Besucher Guided Tours und Topic Routen. Daneben bietet die it-sa eine Fülle an hochwertigen Veranstaltungen wie das it-sa Symposium Banken, den BSI-Grundschutztag, ein Bitkom Embedded Security Forum oder auch den Cisco/Secaron Healthcare-Kongress. Viele weitere Schulungen, Tutorials und Seminare runden das Angebot ab.

Foren und Diskussionsrunden

Die bewährten offenen Foren in den Ausstellungshallen bleiben auch in Nürnberg ein Kernelement der it-sa: Auf zwei Vortragsbühnen teilen Experten dort in zumeist 15-minütigen Kurzvorträgen ihr Fachwissen mit den Besuchern. Zudem finden jeden Tag unter dem Motto „drei Tage - drei Hacker" Live-Hacking-Vorführungen statt. Eine weitere „bekannte Größe" sind die Diskussionsrunden im roten Forum zur Mittagszeit und zum Abschluss des Programmtags: Jeweils um 12 Uhr erörtert <kes>-Chefredakteur Norbert Luckhardt mit zwei Fachleuten zukunftsträchtige Themen zur Informationssicherheit (ISi). Am Dienstag geht es dabei unter der Überschrift „Wie sag ichs meinem Kinde?!" um die Vermittlung von ISi-Wissen und -Bewusstsein, Mittwoch steht die gesellschaftliche Verantwortung der IT auf dem Programm: „Wie die IT, ihre Dienste und deren (Un-)Sicherheit unsere Welt verändern". Und am Donnerstag heißt es: „Heiter bis wolkig? In the Cloud - und dann?!"

it-sa Auditorium

Neu ist ein drittes offenes Podium in den Messehallen: Das it-sa Auditorium beherbergt Sessions, die eine oder mehrere Stunden umfassen und so ein konkretes Thema in größerer Tiefe ausloten als die Kurzvorträge der Foren Rot und Blau. Unter anderem werden dort verschiedene Studien und ihre Ergebnisse vorgestellt. Beispielhaft seien genannt: das (ISC)²-Panel „Ist die IT-Security auf dem Holzweg?" und die TeleTrust Veranstaltung zum Thema „Trusted Security Services".

Das vollständige Programm finden Sie online auf www.it-sa.de.

AUSSTELLERPORTAL it-sa NÜRNBERG 13.–15. OKTOBER 2009

Sicher gegen Datendiebe

Mobile Geräte wie Laptops oder Smartphones bieten viele Einfallstore für den Datendiebstahl. Sicherheitslösungen können dies verhindern – wenn man sie anwendet.

VON ANNA KATHARINA FRICKE

Das Bedrohungspotential durch Datenverlust ist mittlerweile größer als viele andere Gefahren des Internets. Fahrlässigkeit oder Unachtsamkeit spielen bei Datenskandalen oft eine große Rolle. Beispiele aus der letzten Zeit, wie der gestohlene Laptop von Fußballtrainer Christoph Daum mit brisanten Themen aus der Fußballszene oder die anhaltende Serie von Datenpannen der britischen Regierung, gelangen immer wieder in den Mittelpunkt der Öffentlichkeit.

Aber auch der gezielte Datenklau ist auf dem Vormarsch: Im Bereich der Wirtschaft zielen Datendiebe auf technologische Errungenschaften ab. Das Bundesinnenministerium schätzt die verursachten Schäden auf rund 20 Milliarden Euro pro Jahr. Am stärksten betroffen sind Unternehmen aus den Bereichen Anlagen- und Maschinenbau. Immer häufiger werden auch Umwelttechnologien ausspioniert. Als Grund sieht der Verfassungsschutz unter anderem die Naivität der Unternehmen. Viele Firmen sind sich der Risiken, insbesondere im Bereich der Datensicherheit mobiler Geräte nicht bewusst und glauben noch immer, Spionage komme in Filmen und nicht bei ihnen vor.

Dabei öffnen insbesondere mobile Endgeräte wie Laptops, Smartphones oder Blackberrys Schlupflöcher, durch die hochsensible Informationen leicht in die falschen Hände gelangen können. Zwar sind die mobilen Geräte aus dem Unternehmensalltag nicht mehr wegzudenken, gehen Mitarbeiter allerdings mit unternehmenssensiblen Daten auf Reisen, läuten bei den IT-Verantwortlichen der Unternehmen die Alarmglocken. Denn die Geräte entziehen sich unterwegs der Kontrolle des Sicherheitsbeauftragten.

Notebooks beispielsweise können schnell verloren gehen oder werden gestohlen. In unbeaufsichtigten Momenten können sie angezapft werden oder beim Arbeiten über drahtlose Internetverbindungen Hackerangriffen leicht zum Opfer fallen. Insbesondere Hotspots an Bahnhöfen oder Flughäfen stellen oftmals unsichere Internetverbindungen dar, über die niemals sensible Daten versand werden sollten.

Um die Sicherheitsrisiken zu minimieren, sollten Unternehmen die mobilen Geräte in eine umfassende Sicherheitsstrategie einbinden und die Mitarbeiter über bestehende Risiken aufklären. Zur Einhaltung grundlegender Sicherheitsregeln gehören zunächst schwer zu knackende Passwörter mit einem Mix aus mindestens acht Ziffern, Buchstaben und Sonderzeichen. Im Idealfall sollten Passwörter in regelmäßigen Abständen geändert werden. Auch der Ruhemodus muss abgesichert sein. Beim Wechsel in den Arbeitsmodus sollte das Passwort erneut abgefragt werden. Einen weiteren Schutzwall bieten moderne Sicherheitslösungen, bei denen das Passwort vor und nicht erst nach dem Booten abgefragt wird. Dies verhindert, dass ein unbefugter Dritter an das Betriebssystem gelangt, und von dort aus auch Zugriff auf sensible Daten erhält.

Für Behörden und Unternehmen mit besonderen Sicherheitsanforderungen genügen Passwörter allein jedoch nicht mehr. Hier können Smartcards oder Tokens zum Einsatz kommen, die zusätzliche Informationen abfragen, die erst in Verbindung mit dem Passwort des Benutzers das Notebook freischalten. Der Einsatz biometrischer Daten zur Authentisierung wird hier in Zukunft an Bedeutung gewinnen.

Außerdem ist eine automatische und vollständige Verschlüsselung sämtlicher Daten auf der Festplatte eines Notebooks unverzichtbar. So kann zum Beispiel auch ein virtuelles Laufwerk, ein sogenannter versteckter Container, eingerichtet werden, der mit einem Extra-Passwort geschützt ist. Vertrauliche Daten sind dort sehr sicher. Selbst wenn das Passwort geknackt wird, findet der Angreifer noch längst nicht die versteckten Daten. Es öffnet sich eine Alibidatei, während die sensible Datei, ohne nachweisbaren Speicherplatz einzunehmen, im Verborgenen bleibt.

Wird der Laptop entwendet, bieten sich verschiedenen Anti-Diebstahl-Tools an. Mit einer Tracking-Software kann das Gerät lokalisiert werden, sobald es sich mit dem Internet verbindet und dann in Zusammenarbeit mit lokalen Polizeibehörden dem Eigentümer zurückgebracht werden. Vorher können per Fernzugriff vertrauliche Daten gelöscht werden, die Hardware unbrauchbar gemacht oder der Zugriff gesperrt werden. Findet das Gerät den Weg zum Eigentümer zurück, kann dieser den Schutz aufheben und das System mit einem speziellen Passwort neu booten.

Ein besonderes Sicherheitsrisiko stellen Smartphones, PDAs und Blackberrys dar. Zum einen gehen Nutzer mit den handlichen Mobilgeräten in der Regel nachlässiger um als mit ihren Notebooks: Da die Geräte stets griffbereit sind, bleiben sie auch öfter einmal in der Bahn, am Flughafen, im Taxi oder im Restaurant liegen. Zum anderen nutzen nur wenige Anwender Sicherheitsvorkehrungen wie Verschlüsselung und Virenschutz. Gleichzeitig speichert jeder zweite Manager alle möglichen Arten von Informationen wie technische Produkt- und Vertriebsinformationen sowie Kundendetails auf den kleinen Minicomputern.

Hinzu kommt, dass laut einer Studie 73 Prozent der mobilen Anwender nicht wissen, wo die mobilen Sicherheitsrisiken liegen. Nahezu 30 Prozent gaben zu, mobile Sicherheitsrisiken kaum jemals zu berücksichtigen. Und auch die grundlegendste Sicherheitsvorkehrung ist für die Nutzer offenbar alles andere als selbstverständlich: Jeder zweite IT-Security-Verantwortliche gibt zu, bei seinem eigenen Mobilgerät nicht immer ein Kennwort zu verwenden.

Ein Einfallstor für Datendiebe ist zudem die Bluetooth-Verbindung. Nur wenige klicken sich direkt nach dem Kauf eines neuen Gerätes durch das Menü und stellen Bluetooth ab. Wer sein Handy aber auch nur ein Mal für wenige Minuten unbeaufsichtigt liegen lässt, läuft schon Gefahr, dass Datendiebe die Funkstrecke wie eine Standleitung nutzen, die sie jederzeit anzapfen können. Wenige Momente reichen, um fremde Geräte miteinander zu koppeln und die Verbindung auf „dauerhaft akzeptieren" zu konfigurieren.

Dabei können spezielle Sicherheitskarten auch in Mobiltelefonen den Schutz vor einem Fremdzugriff gewährleisten: So muss sich der Nutzer gegenüber der Karte authentisieren, ansonsten wird der Zugriff auf das Mobilgerät verweigert. Außerdem können die Karten die Verschlüsselung des E-Mail-Verkehrs auf der kompletten Übertragungsstrecke zwischen Sendern und Empfängern übernehmen. Optional wird auch der gesamte Speicherinhalt des Mobilgerätes in das Sicherheitskonzept einbezogen und unter Zuhilfenahme der Sicherheitskarte verschlüsselt.

Um ein Mobilgerät im Falle eines Verlustes lahmzulegen, können weitere Sicherheitslösungen greifen. Schickt man eine verstecke SMS an das Gerät, wird der Zugang zu dem System solange gesperrt, bis der rechtmäßige Besitzer ein Passwort eingibt, das er zuvor festgelegt hat. Alternativ kann durch eine SMS auch der gesamte Arbeitsspeicher gelöscht werden. Sensible Informationen müssen also nicht in falsche Hände geraten – vorausgesetzt man hat sich vorher gewappnet.

Individuelle Sicherheit für Smartphones

Smartphones unterstützen Mitarbeiter quer über alle Hierarchiestufen bei ihrer Arbeit im Geschäftsalltag. Im Gegensatz zu Notebooks sind sie allerdings nicht immer in die IT-Sicherheitskonzepte integriert. Mit der Mobile Security Card von Giesecke & Devrient lassen sich Smartphones sicher in die Unternehmens-IT einbinden und Sicherheitsrisiken minimieren.

Klein und handlich hält der Siegeszug der Smartphones an. Sie etablieren sich neben den Notebooks zum Standardinventar für den Geschäftsalltag. Die Funktionen der Geräte, seien sie von Nokia, BlackBerry-Hersteller RIM oder HTC, im mobilen Office-Alltag wachsen stetig. Mit ihnen können Geschäftsleute heute nicht mehr nur E-Mails austauschen oder den Kalender pflegen, sondern auch auf wichtige Daten mithilfe mobiler Software-Programme (z.B. SAP, Standard-Office-Anwendungen) auf Firmennetzwerke zugreifen, wie es bisher nur mit Notebooks möglich war. Die Vorteile mobiler Lösungen sind eindeutig: Mitarbeiter können mithilfe der Geräte noch schneller auf interne und externe Kundenanfragen reagieren, Unternehmen werden damit schlagkräftiger.

Der Smartphone-Einsatz im Geschäftsalltag birgt allerdings nicht nur Chancen, sondern auch Risiken. Während sich bei Notebooks über das letzte Jahrzehnt hinweg eine funktionierende sichere Infrastruktur entwickelt hat und sie in das individuelle IT-Sicherheitskonzept von Unternehmen eingepasst sind, ist dies bei Smartphones bisher oft nicht der Fall. Heutige Smartphone-Plattformen bieten zwar schon ein Maß an Sicherheit, vielfach lassen sie sich allerdings nicht an die individuelle Sicherheitsarchitektur der Unternehmen anpassen und kontrollieren.

G&D-Lösung für BlackBerry

Hier kommt die „Mobile Security Card" von Giesecke & Devrient (G&D) ins Spiel. Die Smartcard von G&D wird dazu in den microSD-Kartensteckplatz des Smartphones eingesetzt und gewährleistet als unabhängiges Kryptomodul Nutzerauthentisierung, hochsichere E-Mail-Verschlüsselung und sicheren Zugriff auf Unternehmensnetze – je nach den individuellen Sicherheitsanforderungen des Unternehmens. G&D bietet bereits eine Sicherheitslösung für BlackBerry Smartphones von RIM auf Basis der Mobile Security Card an.

Unternehmensführung und Risikomanagement

VON DR. WOLFGANG BÖHMER

Sind schwarze Schwäne in der IT denkbar?

Schwarze Schwäne sind ein Sinnbild für Ereignisse, die eigentlich nicht eintreten dürften, denn sie liegen außerhalb unserer Vorstellung und Erfahrung. Bevor Australien entdeckt wurde, waren die Menschen davon überzeugt, dass alle Schwäne weiß seien. Diese Überzeugung wurde durch empirische Evidenz geprägt. Als der erste schwarze Schwan gesichtet wurde, fiel das bisherige Gedankengebäude zusammen.

Die Schwarze-Schwan-Illustration veranschaulicht eine schwerwiegende Beschränkung bei unserem Lernen durch Beobachtung oder Erfahrung und zeigt die Zerbrechlichkeit unseres Wissens.

Leider verlassen sich in der Praxis des IT-Risikomanagements noch zu viele „Experten" auf den Blick in den Rückspiegel und ins „Logbuch". Oder häufig setzen Unternehmen auf eine reine Bedrohungs- oder Gefährdungsanalyse. Diese Praktiken haben mit einer zukunftsorientierten Risikoanalyse nichts zu tun und werden einem IT-Risikomanage-ment nicht gerecht. Komplementär zum Risiko steht die Sicherheit (Risiko = 1 – Sicherheit). Wird die eine Größe verringert, geht dies zu Lasten der anderen Größe und umgekehrt. Risikomanagement muss sich auf potenzielle Zukunftsszenarien konzentrieren und darf sich nicht auf die Erklärung der Vergangenheit beschränken.

Es ist absehbar, dass sich traditionelle Risikomanagementsysteme zu „ganzheitlichen" Unternehmenssteuerungssystemen weiterentwickeln. IT-Risikomanagement wird integraler Bestandteil von wertorientierten Steuerungssystemen. Denn stochastische Szenarioanalysen ermöglichen einen besseren Blick auf mögliche Zukunftspfade. Die Zukunft gehört modernen, dynamischen Bewertungs- und Steuerungsmethoden, beispielsweise Simulationsverfahren. In diesem Zusammenhang werden sich auch die klassischen (deterministischen) Methoden des Risikomanagements stark weiterentwickeln müssen. Rückversicherungsunternehmen, Technologiekonzerne und Ingenieure wenden diese modernen Methoden bereits heute an. Denn sie sind in der Lage mittels quantitativer Risikomethoden z.B. die Auswirkungen einer 100-jährigen Welle für den Bau einer Ölplattform zu kalkulieren. Oder sie kalkulieren den Kapitalbedarf in der Folge eines Hurrikans, der über die Karibik fegt. Alternativ kann auch – mit Hilfe von stochastischen Szenarien untersucht werden, welche Auswirkung der Ausfall eines hochverfügbaren IT-Systems auf das Finanzergebnis haben wird. Ergänzend kann die Insolvenzwahrscheinlichkeit berechnet werden. Und allen Methoden liegt eine schlichte Frage zu Grunde, die vor allem auch in der Informations- und Kommunikationstechnologie von hoher Relevanz ist: Wie schief kann es denn gehen, wenn etwas schief geht?

„Neue Technologien brauchen Sicherheit"

Oliver Grün ist Vorsitzender des VDEB Verband IT-Mittelstand e.V. und Vorstand der GRÜN Software AG. Er weist darauf hin, dass die zunehmende Komplexität der IT-Systeme auch unter Sicherheitsaspekten gesehen werden muss. Wenn das Vertrauen in eine sichere Infrastruktur abhanden kommt, haben neue webbasierte Technologien kaum eine Chance.

Worin sehen Sie die derzeit wichtigsten Entwicklungen in der IT-Sicherheit?

Wir können für die Zukunft eine rasant ansteigende Komplexität der IT-Systeme erwarten. Diese Komplexität bietet in vielfältiger Weise Angriffsstellen. Neue Technologien werden sich aber nur dann durchsetzen, wenn Vertrauen in ihre Sicherheit besteht. Besonders beim Cloud Computing ist dies ersichtlich. Die Auslagerung und der vernetzte Zugriff auf kritische Unternehmensdaten lässt Bedenken entstehen, die nur mit überzeugenden Lösungen ausgeräumt werden können. Ingesamt denke ich, dass der Stellenwert der IT-Security bei den Unternehmen angekommen ist, denn auch in der Wirtschaftskrise hat sich der Security-Markt als robust erwiesen.

Was sind Ihrer Meinung nach die besten Abwehrmaßnahmen gegen IT-Angriffe?

Zunächst ist das fachliche Know-how qualifizierter Mitarbeiter gefragt, die auf dem neuesten Stand der Technik sind und die kriminellen Aktivitäten beispielsweise in Form von Computerviren, schädlichen Links und PDFs, SQL-Injection- und Phishing-Attacks oder Trojanern intensiv verfolgen, um entsprechende Abwehrmaßnahmen präventiv vorzunehmen. Ein guter IT-Sicherheitsleiter wird aber gleichzeitig nicht nur rein technische Lösungen entwickeln, sondern das Unternehmen insgesamt in den Blick nehmen und ein Informationssicherheitsmanagement entwickeln.

Was gehört zu einem solchen Management dazu?

Hierzu gehört beispielsweise die Klassifikation von Daten gemäß ihrer Wichtigkeit oder die verbindliche Festlegung von Sicherheitsregeln. Diese müssen dann allerdings auch den Mitarbeitern in Schulungen vermittelt werden. In der Hitze des geschäftlichen Alltags werden Sicherheitsregeln gerne vernachlässigt, ohne dass eine böswillige Absicht besteht. Die spektakulären Fälle von illegalem Datenhandel und Datenklau zeigen, dass die Daten nicht mit aufwendigen technischen Systemen entwendet wurden, sondern mittels USB-Stick oder CD-Rom.

Was können Sie als IT-Mittelstandsverband für eine sichere IT leisten?

Wir können zum Beispiel aus mittelständischer Sicht darauf hinweisen, dass auf politischer Ebene die Standardisierung von elektronischen Systemen und Sicherheitsbestimmungen international vorangetrieben werden muss, um die Komplexität zu beherrschen und besonders neuralgische Punkte wie die beispielsweise die webbasierten Zahlungssysteme zu schützen. Damit bieten wir mittelständischen Unternehmen die Möglichkeit, ihr Gesicht zu zeigen und sich Gehör zu verschaffen – nicht gegenüber der Politik, sondern auch gegenüber den IT-Konzernen.

Daten immer sicher im Gepäck: Virtualisierungstechnik auf Reisen

VON DR. RAINER BAUMGART, Vorstandsmitglied im TeleTrusT Deutschland e.V.

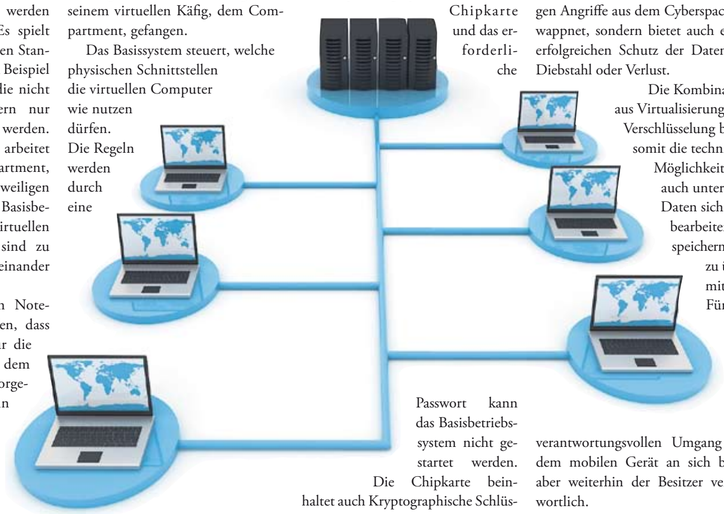
Die auf Notebooks gespeicherten Informationen sind größeren Gefahren ausgesetzt, als die Daten auf stationären Arbeitsplätzen. Denn neben unsicheren öffentlichen Netzzugängen und zahlreichen Angriffsflächen über Funkschnittstellen existiert auch noch das Risiko von Verlust oder Diebstahl. Die Absicherung gegen all diese Gefahren darf aber nicht auf Kosten der Mobilität geschehen und muss dem Mitarbeiter weiterhin ein unkompliziertes Arbeiten erlauben.

Ein Lösungsansatz, der diesen Anforderungen gerecht wird, ist die Virtualisierungstechnik. Sie bietet den Benutzern die Möglichkeit, weiterhin in ihrer vertrauten Umgebung und mit ihren Standardprogrammen zu arbeiten. Dabei ist so ein System leicht zu bedienen und kann auf einem Standard-Notebook betrieben werden und bietet gleichzeitig höchsten Schutz.

Wie funktioniert die Virtualisierung und was macht das mobile System so sicher? Der Ausgangspunkt ist ein schlankes Basisbetriebssystem von dem angenommen werden kann, dass es sicher ist. Es spielt einem oder mehreren anderen Standard-Betriebssystemen, zum Beispiel Windows, Computer vor, die nicht physisch existieren, sondern nur von der Software abgebildet werden. Jeder Software-Computer arbeitet in einem eigenen Compartment, das heißt, die Daten des jeweiligen virtuellen Computers, des Basisbetriebssystems, sowie der virtuellen Computer untereinander, sind zu jedem Zeitpunkt strikt voneinander getrennt.

In der Praxis kann ein Notebook so eingerichtet werden, dass ein virtueller Computer für die sichere Verbindung mit dem Unternehmensnetzwerk vorgesehen ist und zeitgleich ein anderer virtueller Computer vom Anwender für das Internet genutzt wird. Sollte sich der virtuelle Internet-Computer mit Schadsoftware infizieren, bleibt das Unternehmensnetzwerk davon unbehelligt, denn der Schädling ist in seinem virtuellen Käfig, dem Compartment, gefangen.

Das Basissystem steuert, welche physischen Schnittstellen die virtuellen Computer wie nutzen dürfen. Die Regeln werden durch eine Sicherheitsrichtlinie festgelegt und auf einem getrennten Medium, einer Chipkarte, gespeichert. Ohne die Chipkarte und das erforderliche Passwort kann das Basisbetriebssystem nicht gestartet werden. Die Chipkarte beinhaltet auch Kryptographische Schlüssel, die für die vollständige Verschlüsselung der Festplatte genutzt werden. Damit ist so ein System nicht nur gegen Angriffe aus dem Cyberspace gewappnet, sondern bietet auch einen erfolgreichen Schutz der Daten bei Diebstahl oder Verlust.



Die Kombination aus Virtualisierung und Verschlüsselung bietet somit die technische Möglichkeit, um auch unterwegs Daten sicher zu bearbeiten, zu speichern und zu übermitteln. Für den verantwortungsvollen Umgang mit dem mobilen Gerät an sich bleibt aber weiterhin der Besitzer verantwortlich.

„Compliance-Anforderungen gerecht werden“

Immer mehr Unternehmen suchen einen ganzheitlichen Lösungsansatz für IT-Security, Compliance und IT-Governance, meint Tom Köhler, Direktor Strategie Informationssicherheit & Kommunikation bei der Microsoft Deuschland GmbH. Mit Standard-Software will der Konzern seinen Kunden helfen, ihre vielfältigen Geschäftsanforderungen kostengünstiger zu lösen.

Welchen Bedarf sehen Sie derzeit in puncto IT-Security in den Unternehmen?

IT-Security gilt heute nicht mehr als Einzeldisziplin. Unsere Kunden betrachten IT-Security, Compliance und IT-Governance zunehmend als ein Konvergenzthema. Der Bedarf an einem ganzheitlichen, integrierten Lösungsansatz ist dementsprechend größer geworden. Dieser Trend wird durch die wirtschaftliche Lage noch beschleunigt. Es ist notwendig, sich von Silo-Projekten zu verabschieden und mehr Synergie-Effekte aus der vorhandenen Infrastruktur herauszuholen.

Inwiefern können Sie denn beim Aufbau von Compliance-Vorgaben unterstützen?

Wir helfen unseren Kunden, ihre Geschäfts- und Compliance-Anforderungen durch unsere Standard-Software kostengünstiger zu lösen. Um ein Praxisbeispiel zu nennen: Kunden können mit unserem SharePoint Server ihre elektronischen Geschäftsunterlagen rechts- und revisionssicher archivieren. Uns ist bewusst, dass Microsoft oft nicht im Compliance Umfeld wahrgenommen wird. Daher werden wir in diesem Jahr das Thema intensiver bei unseren Kunden und Partnern ansprechen.

Wie denken die IT-Verantwortlichen über Compliance?

Meine Erfahrung aus Kundengesprächen ist, dass durch den inflationären Gebrauch und die häufig mangelhafte Definition der Begriff Compliance auf den verschiedenen Ebenen der IT-Verantwortlichen zu Verwirrung führt. Im vergangenen Jahr haben wir in einer Studie herausgefunden, dass nur zehn Prozent der IT-Verantwortlichen gegenüber 41 Prozent der Business-Ansprechpartner sagten, dass sie sehr zufrieden mit der Umsetzung von Compliance-Anforderungen in Ihrem Verantwortungsbereich seien. Es besteht also immer noch eine zu große Kluft zwischen dem IT-Verantwortlichen und den Unternehmenslenkern.

Welche konkreten Probleme werden seitens der IT-Verantwortlichen geäußert?

Einerseits fehlt ein gemeinsames Verständnis über Compliance bei IT- und Business Managern. Andererseits nehmen die regulatorischen Anforderungen an die IT-Infrastruktur weiter zu. Beispiele sind das neue Datenschutzgesetz oder die Datenvorratsspeicherung. Die Komplexität des Themas erfordert zunehmend eine abteilungsübergreifende Sicht. Als Hilfestellung haben wir ein Plattform-neutrales IT-Infrastruktur Compliance Reifegradmodell entwickelt, um Unternehmen die Nutzenpotentiale aufzuzeigen und gleichzeitig eine Basis für das gemeinsame Verständnis zu schaffen.

Identitätsnachweis per elektronischem Personalausweis

Neue Techniken für elektronische Identitäten

Eine elektronische Identität soll Mensch oder Maschine, Organisationseinheit oder Kommunikationskomponente sicher und zuverlässig in der digitalen Welt abbilden. Um sichere elektronische Geschäftsprozesse zu gestalten, muss eine Vielfalt organisatorischer Rollen (z.B. Mitarbeiter, Kunde, Lieferant) oder aber technischer Komponenten (z.B. LKW Onboard Unit, elektronischer Fahrausweis oder IP Router) abgebildet werden.

Die PKI (Public Key Infrastructure) Technologie bietet die Möglichkeit, alle denkbaren Entitäten exakt nach Bedarf und Anwendungsfeld zu modellieren und in digitalen Zertifikaten abzubilden. Die Bandbreite der Zertifikatsinhalte reicht dabei vom personenbezogenen elektronischen Mitarbeiterausweis bis hin zur vollständig anonymisierten Identifikationsnummer. Je nach Gefährdungslage und Sicherheitsanforderung kann das Zertifikat auf einer SmartCard, auf einem Hardware Token oder auch als Softwaretoken ausgegeben werden. Dasselbe Zertifikat kann parallel in verschiedenen Anwendungen genutzt werden und bietet den Mehrwert, neben der Authentifizierung der Kommunikationspartner auch die Vertraulichkeit und Authentizität ausgetauschter Informationen durch Verschlüsselung und Signatur sicherstellen zu können. Moderne PKI Plattformen sind flexibel und schnell einsetzbar und lassen sich einfach in beliebige Arten von Anwendungen integrieren.

Ab November 2010 wird in Deutschland ein weiteres vielversprechendes Medium zum Identitätsnachweis in Gestalt des elektronischen Personalausweises (ePA) vorhanden sein. Dieser Ausweis im Scheckkartenformat enthält einen kontaktlosen Chip, der vom Gesetzgeber definierte Zusatzfunktionalitäten erbringt. Sind die notwendige Clientsoftware sowie ein Kartenleser beim Bürger vorhanden, können persönliche Daten wie Name oder Adresse im Rahmen von Online Anwendungen vom Ausweis gelesen werden. Ebenso ist eine Altersverifikation sowie eine Nutzung als sicherer Login/Passwort Ersatz möglich. All diese Funktionalitäten benötigen die explizite Zustimmung des Bürgers durch Eingabe einer PIN. Diensteanbieter, die diese neuen Möglichkeiten in ihren Onlineprozessen nutzen möchten, benötigen einen eID-Server, der Anwendungen entlastet, indem er die erforderlichen komplexen Kommunikationsabläufe und Anbindungen sicherheitstechnischer Funktionen übernimmt.

Als Fazit bleibt festzuhalten, dass neben dem elektronischen Personalausweis (ePA) mit nur nationaler Anwendbarkeit und fest vorgegebenen Nutzungsszenarien die bewährte PKI Technologie mit ihren deutlich flexibleren Möglichkeiten auch weiterhin eine wesentliche Rolle bei der elektronischer Identitätsbildung behalten wird.

mtG: Der Spezialist für PKI Aufbau und Anwendungen des elektronischen Personalausweises

mtG bietet seinen Kunden die folgenden Produkte und Dienstleistungen:

PKI-Aufbau

mtG ist spezialisiert auf Konzeption und Aufbau von PKI Infrastrukturen bei Unternehmen, Behörden oder Trust Centern. mtG verfügt dabei über 12 Jahre Praxiserfahrung in zahlreichen Großprojekten.

Das von mtG entwickelte PKI Produkt mtG-CARA ist ein flexibel konfigurierbares, mandantenfähiges CA-System zur professionellen Erzeugung und Verwaltung von X.509 und CV Zertifikaten. Es zeichnet sich durch hochgradige Skalierbarkeit, Performanz und Verfügbarkeit sowie integrierte Funktionalitäten einer Registration Authority (RA) aus. mtG-CARA erlaubt die problemlose Integration der PKI Funktionalitäten in Unternehmens- oder Behördenabläufe, z.B. auch in SOA Architekturen. Unsere Experten beraten und unterstützen professionell bei der Systemintegration.

mtG-CARA ist u.a. bei einem der großen Trust Center Deutschlands und bei einer Reihe von Versicherern im Wirkbetrieb.

Nutzung der eID Funktion des elektronischen Personalausweises (ePA)

mtG Mitarbeiter sind hochqualifizierte Sicherheitsexperten, und verfügen durch mehrjährige Mitarbeit in Pilotprojekten über ausgezeichnetes technisches Know-How zu den eID Funktionalitäten des künftigen elektronischen Personalausweises.

mtG wird gemeinsam mit einem Entwicklungspartner in Kürze einen eID Server bereitstellen. Dieser ermöglicht über einfach zu nutzende Schnittstellen das Auslesen von Personendaten, die Altersverifikation und die Identifikation per Personalausweis. Firmen können damit die Zeit bis zur Einführung des neuen Ausweises Ende 2010 zur Konzeption, Realisierung und Erprobung ePA basierender Anwendungen nutzen.

Unsere Experten stehen schon jetzt für Beratung und Unterstützung bereit.

Besuchen Sie uns auf der Sicherheitsmesse it-sa in Nürnberg vom 13. bis 15.Oktober 2009,

in Halle 6 Stand 6-541

media transfer AG (mtG)
Dolivostraße 11
D-64293 Darmstadt
Telefon: +49 6151 8193-0
Fax: +49 6151 8193-43
contact@mgt.de
www.mtg.de

Achtung, Wirtschaftsspionage!

Webapplikationen auf Unternehmensseiten sind oft ungeschützt und damit Top-Ziel für Spione und Hacker

Wer bei Web-Sicherheit denkt, dass mit Secure Layers (SSL), Firewalls oder Sicherheitsmechanismen für Netzwerke und Host-Computer schon alles getan ist, irrt. Wie der aktuelle X-Force Report von IBM zeigt, werden Webanwendungen immer häufiger zum Angriffsziel von Wirtschaftsspionen und Hackern. Während klassische Arbeitsplatzrechner häufig gut durch Virenscanner geschützt sind, stehen Webapplikationen vor Hackern relativ ungeschützt da. Eine Tatsache, die bereits einigen Organisationen zum Verhängnis wurde.

Am letzten Tag im Juli war es soweit: Online-Gamer sollten den Startschuss der ersten Online-Spielemesse live im Internet miterleben und einige der Spiele gleich am Bildschirm ausprobieren können. Was sich die Macher der ‚Games Convention Online‘ so schön vorgestellt hatten, fiel buchstäblich aus. Ausgerechnet die Webseite, die mit virtuellem Rundgang und Spielen glänzen sollte, war am Eröffnungstag nicht zugänglich. Was höchstwahrscheinlich das Resultat eines Hackerangriffs war, ist inzwischen kein Einzelfall mehr.

Laut des halbjährlichen X-Force Report von IBM schnellten kriminelle Angriffe auf Webanwendungen im vergangenen Halbjahr in die Höhe. So sind beispielsweise die so genannten SQL Injection Attacken, bei denen Hacker schadhaften Code in Unternehmens-Webseiten einspeisen, um deren Besucher zu infizieren, vom letzten Quartal 2008 bis zum Ende des ersten Quartals 2009 um 50 Prozent gestiegen. Von Q1 bis Q2 2009 hat sich die Zahl dieser Angriffe bereits fast verdoppelt.

Damit steht fest, dass Web-Sicherheit keinesfalls ausschließlich eine Browser oder Client-seitige Angelegenheit ist. Webanwendungen, also die Anwendungen, die den Austausch zwischen dem internetfähigen Computer zuhause mit jeder beliebigen Webseite bzw. dem zugehörigen Webserver ermöglichen, sind aufgrund ihrer Mehrschichtigkeit für Angriffe besonders anfällig. Jede Nachricht, die damit gestartet wird, dass ein Nutzer in seinem Webbrowser die Adresse der Internetseite seiner Wahl eingibt, durchläuft mehrere Netzwerkprotokollschichten. Bei jeder weiteren Interaktion des Users werden Daten vom Browser bis in die Backend-Systeme durchgereicht und das Ergebnis zurückgegeben. Schwachstellen in einer einzigen der verschiedenen Schichten stellen nicht nur ein erhebliches Sicherheitsrisiko für das gesamte Unternehmen dar, sondern können zum Beispiel bei Online-Shops sogar existenzgefährdend sein.

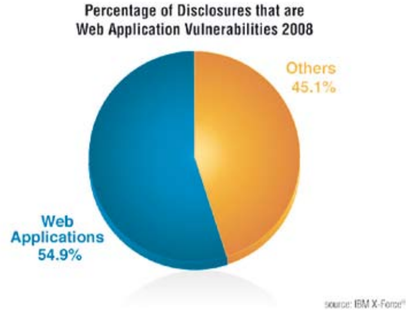
Hier setzen nur durchgängige Lösungen an, die nicht nur alle Bereiche unter die Lupe nehmen, Schwachstellen identifizieren und „verarzten“, sondern die langfristig auch die Entwickler sensibilisieren. Denn: Sicherheit sollte bereits in der Entwicklung ansetzen - je früher, desto günstiger.

Sicherheit von Anfang an

Moderne Tools durchleuchten Web-Anwendungen nach Schwachstellen und unterstützen das Management bei der Einhaltung von Sicherheitsrichtlinien – vom Entwurf bis zum Produktivbetrieb.

Es ist der Alptraum jedes Unternehmens, wenn die eigene Website Schädlinge wie Viren und Trojaner an Besucher verteilt oder vertrauliche Kundendaten an Kriminelle weiterleitet. Firewalls und Überwachungsmaßnahmen im laufenden Betrieb schützen davor kaum, solange die Webanwendung Sicherheitsmängel aufweist.

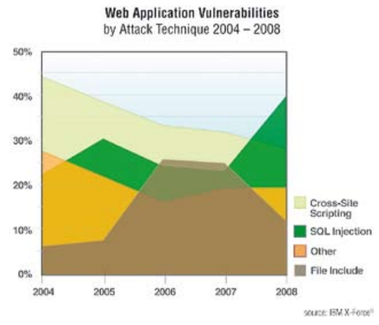
Zwei Sätze, die jeder CIO und jeder Entwicklungsleiter unterschreiben würde, lauten so: „Sicherheit muss Chefsache sein“ und „Ein Sicherheitskonzept muss alle Phasen des Software-Lebenszyklus umfassen“ Dies in die Praxis umzusetzen, ist aber keineswegs trivial, schließlich sind Entwickler nicht unbedingt Security-Experten. Doch Sicherheitslücken, die in einer frühen Phase des Entwicklungszyklus in die Anwendung geraten und es unbemerkt bis in die Produktivphase schaffen, kommen ein Unternehmen teuer zu stehen: Etwa 30mal mehr kostet es dann, einen Fehler auszumerzen – Umsatzausfälle, aufwändige Datenrettungsaktionen oder sonstige Folgekosten noch gar nicht eingerechnet.



Früherkennung spart Folgekosten.

Hier setzen Testwerkzeuge wie IBM Rational AppScan an, die von der Entwurfsphase bis zum Produktivbetrieb einen einheitlichen Blick auf die Sicherheit bieten und frühzeitig auf Probleme hinweisen. AppScan verhält sich wie ein Security-Experte, der alle Tricks kennt und die Web-Applikation aus der Perspektive des Nutzers – oder Angreifers – auf Schwachstellen abklopft.

Es liegt in der Natur von Webanwendungen, dass die Grenzen zwischen Code und Daten fließend sind. Schadcode kann sich in der Datenbank verbergen, eingeschleust durch SQL-Injections, in Flash-Anwendungen oder von Nutzern hochgeladenen JPEG-Bildern. AppScan folgt dem Weg eines HTTP-Requests bis tief hinein in die innersten Strukturen der Daten und des Codes, stellt Probleme fest und macht Lösungsvorschläge. Fast wie nebenbei schärft es auch das Sicherheitsbewusstsein im Entwickerteam: Im Kontext jeder aufgefundenen Schwachstelle stellt AppScan direkt in der Bedienoberfläche Tutorials zur Verfügung, die das Verständnis der Entwickler für diese Lücke und ihre Auswirkungen vertiefen.



Dabei ist die Oberfläche bewusst übersichtlich gehalten und nicht nur für Techniker gedacht. Manager und Projektleiter können sich jederzeit einen Überblick über den Sicherheitszustand des Projekts verschaffen, ohne sich in Details zu verlieren. Andererseits erlaubt es das Interface im Bedarfsfall, jedem einzelnen Problem bis auf die Quellcode-Ebene zu folgen.

Security immer im Blick

Report-Generatoren tragen den Bedürfnissen der verschiedenen Stakeholder im Sicherheitskonzept Rechnung. AppScan kann automatisch Berichte erzeugen, die sich speziell an Entwickler, an QA-Experten oder an Executives richten. Hier ragen besonders zahlreiche Vorlagen zu Compliance-Reports nach Richtlinien wie Sarbanes-Oxley, den EU-Direktiven zum Datenschutz wie 2002/58/EC oder den Standards der Payment Card Industry (PCI) heraus.

All das kann zwar das Wissen um die Verwundbarkeit von Web-Anwendungen und ein integratives Sicherheitskonzept nicht ersetzen. Wenn ein intelligentes Werkzeug jedoch hierarchieübergreifend und im gesamten Lebenszyklus zum Einsatz kommt, kann es eines: dieses Konzept als Chefsache und als Sache jedes einzelnen Entwicklers in gelebte Realität verwandeln. Die Nutzer werden es danken und Angreifer leichtere Beute suchen.

Weitere Informationen zu Security@IBM unter:

www.ibm.com/de/security

„Unternehmen mangelt es an gut ausgebildeten IT-Sicherheitsexperten“

Birgitte Baardseth, Geschäftsführerin der International School of IT Security (isits), weiß, dass hochkarätige Ausbildungen im Bereich von IT-Security und Datensicherheit noch eine Mangelware sind. Gleichzeitig gewinnen Themen wie Datensicherheit und Security-Awareness bei Arbeitgebern und Organisationen an Bedeutung.

Auf welche Bereiche erstreckt sich das Angebot der isits?

Die Schule bietet Aus- und Fortbildungen an, mit dem Ziel Fachleute mit einem erstklassigen Wissen für die Themen rund um IT Security und Informationssicherheit nachweisbar auszustatten. Dazu zählt zum Beispiel das T.I.S.P Zertifikat, ein Expertenzertifikat im Bereich der Informationssicherheit, das auf die speziellen Standards und Gesetzgebungen im Europäischen Raum zugeschnitten ist. Außerdem bieten wir seit 2006 ein berufsbegleitendes Fernstudium in Kooperation mit der Ruhr-Universität Bochum an, das mit dem Grad „Master of Science in Applied IT Security“ abschließt. Hier können Fachleute ihre Kenntnisse in Pflichtmodulen wie Sicherheitsmanagement oder Kryptografie bis hin zu innovativen Wahlfächern wie der IT-Forensik, also der Wiederherstellung von Daten, vertiefen.

Worauf achten Unternehmen bei der Einstellung von IT-Sicherheitsexperten?

Neben dem aktuellen technischen Know-how sind sogenannte „weiche“ Faktoren gefragt. Fachleute müssen beispielsweise auch über die juristischen Aspekte oder den betriebswirtschaftlichen Nutzen von IT-Sicherheit Bescheid wissen. Neben Berufserfahrung spielen akademische Nachweise und praktische Weiterbildung für das Berufsfeld eine wichtige Rolle.

Wie sieht die Nachfrage in den Unternehmen aus?

Die Nachfrage in den Unternehmen ist groß. Viele Unternehmen fragen direkt bei unserer Schule nach IT-Sicherheitsexperten an. Es kommt also häufig vor, dass Studienteilnehmer noch während ihres Studiums attraktive Jobangebote bekommen und ihren Arbeitgeber wechseln. Das liegt daran, dass heutzutage in allen Bereichen elektronisch mit sensiblen Daten gearbeitet wird, von der Krankenhausverwaltung über den Automobilhersteller bis hin zu Behörden. Die Unternehmen sind zunehmend für Themen wie Datensicherheit und Security Awareness sensibilisiert.

Was müssen IT-Experten beim Thema Security Awareness beachten?

Fachleute müssen die IT-Anwender, also die Mitarbeiter des Unternehmens, für mögliche Risiken und Sicherheitslücken sensibilisieren. Denn mehr als 70 Prozent der Bedrohungen stammen nicht von außerhalb, sondern von den Anwendern selber. Dies muss nicht aus krimineller Energie geschehen, sondern vielmehr aus Unwissenheit und Unachtsamkeit. Das gängigste Beispiel ist hier das Computer-Passwort, das direkt am Bildschirm klebt. Zum Thema Security Awareness veranstalten wir daher im Oktober eine internationale Konferenz, bei der sich die Teilnehmer über Vorgehensweise und Kampagnen informieren und austauschen können.

Sicherheit im Unternehmen

Deutscher Mittelstand im Visier von Cyberkriminellen

VON LOTHAR SYMANOFSKY

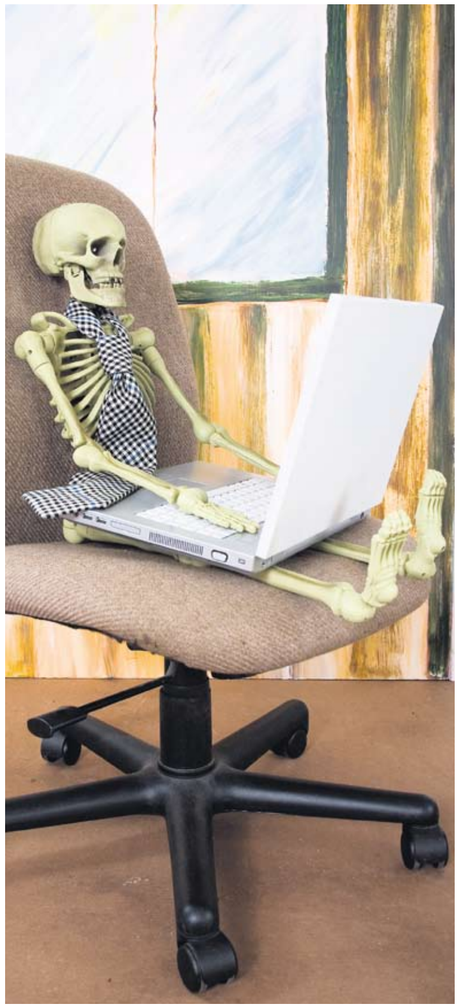
Mehr und mehr gerät der Deutsche Mittelstand ins Visier krimineller Betrüger und Spione, die das Internet dazu nutzen, die Unternehmen auszuhorchen und sich auf deren Kosten zu bereichern. Längst hat sich ein weltweites Netzwerk von Cyberkriminellen gebildet, das, ausgerüstet mit modernsten Computersystemen, mit einem Heer von gut ausgebildeten IT-Experten und nahezu unbegrenzten Kapitalressourcen den deutschen Mittelstand gezielt attackiert.

Statistiken zeigen, dass PC-User weltweit es täglich mit 2.000 neuen Viren und monatlich 50.000 Phishing-Attacken zu tun haben. Hinzu kommt, dass jährlich mehr als 1.000.000 PCs gekapert werden, die selbst wiederum gefährliche Malware verbreiten. Während des ersten Halbjahres 2009 haben die Programmierer von Schadsoftware weiterhin alles darangesetzt, Computer zu infizieren und daraus direkten finanziellen Nutzen zu ziehen oder die Kontrolle über die betroffenen Rechner zu erlangen. Gemäß dem E-Threat-Report von BitDefender sind vor allem Trojaner weiter auf dem Vormarsch. Ihr Anteil an der weltweit erkannten, aktiven Malware beträgt derzeit sage und schreibe 83 Prozent. Cyberkriminelle nutzen immer ausgefeiltere Methoden, um sich den Zugang zu Informationen wie beispielsweise Online-Bankkonten, Kreditkartendaten oder anderen sensiblen Personendaten zu verschaffen. Dazu entwickeln sie in immer kürzeren Intervallen neue Angriffsmethoden und digitale Betrugsmaschen. Beispielsweise machen neuartige Verfahren zur Verschlüsselung von Malware die herkömmlichen, rein signaturbasierten Antivirenprogramme wirkungslos.

Im Kampf gegen die Internetkriminalität sind also neue, innovative Technologien gefragt. Die Idee dahinter: Da ein „digitaler“ Angreifer nicht anhand seines Fingerabdruckes oder Fotos identifiziert werden kann, beobachtet man stattdessen sehr genau das Verhalten der potenziell gefährlichen Software. B-Have (heuristische Verhaltensanalyse in virtuellen Umgebungen) heißt das technologische Stichwort. Dabei handelt es sich, vereinfacht gesagt, um einen virtuellen PC – also einen Computer im Computer. In diesem simulierten Rechner lassen sich ohne Risiko verdächtige Programme oder Dateien, beispielsweise verschlüsselte Malware, ausführen. Deren Aktivitäten werden so auf mögliche Gefahren hin überprüft. Nur wenn die Software als ungefährlich eingestuft wird, kann sie auf dem eigentlichen System ausgeführt werden. Dieses Verfahren bietet mehr Sicherheit und signifikant höhere Erkennungsraten von neuen, unbekannten Threats.

Was aber passiert, wenn sich der Schadcode erst Minuten oder sogar Stunden danach aktiviert? Niemand kann solange auf das Resultat eines Scanners warten – verlässliche Ergebnisse müssen daher in Echtzeit bereitgestellt werden. Um dieses Schlupfloch zu schließen, wurde von Security Software-Ingenieuren von BitDefender ein innovatives Intrusion Detection-System entwickelt. Diese Technik wirkt wie eine Schutzschicht, die sich zwischen dem zu schützenden System und einer unbekannten, potenziell gefährlichen Software legt. Treten Unregelmäßigkeiten im Laufzeitverhalten auf, wird das entsprechende Programm als gefährlich klassifiziert und terminiert bzw. in Quarantäne verschoben. Zahlreiche Tests von unabhängigen Institutionen bescheinigen die Wirksamkeit dieses Verfahrens.

Mit seinen Security Suites for Business (Client Security, Security for Exchange, Security for Mail Server) bietet BitDefender mittelständischen Unternehmen einen wirksamen Schutz vor allen Malware-Bedrohungen. Damit können Unternehmen auf ein robustes und einfach zu bedienendes Paket von Sicherheitsapplikationen zurückgreifen, die speziell für den Schutz komplexer Unternehmensnetzwerke konzipiert wurden und durch eine einfache Administration überzeugen.



So viel Sicherheit wie nötig

Eine Kombination aus technischen Schutzmaßnahmen und umsichtigem Verhalten schützt die IT am besten gegen Viren, Spionageprogramme und Spam-Mails.

VON SARAH WAGNER

Zunächst die gute Nachricht: Laut einer Umfrage des Branchenverbandes Bitkom sind 63 Prozent der deutschen Internetnutzer bislang von negativen Erfahrungen im Internet verschont geblieben. Doch haben 22 Prozent – das entspricht zehn Millionen Bundesbürgern – schon erlebt, dass ihr Computer mit einem Schadprogramm infiziert wurde. Sechs Prozent der Surfer sind nach eigenen Angaben bereits Opfer eines Betrugs beim Online-Einkauf geworden.

Jedoch besitzen die deutschen Internetnutzer ein ausgeprägtes Risikobewusstsein: 95 Prozent kennen die wichtigsten Gefahren im Netz, ergab eine Umfrage im Auftrag der EU. Dazu zählen Viren, Spam, Phishing, Diebstahl von elektronischen Daten oder Identitäten sowie die Möglichkeit, dass der Rechner Teil eines Bot-Netzes wird. „Gegen Schadprogramme und Betrüger können PC-Nutzer vorbeugen“, sagt Bitkom-Präsidiumsmitglied Dieter Kempf. „Mit einer Kombination aus Schutzprogrammen und umsichtigem Verhalten lassen sich viele Risiken effektiv eindämmen.“

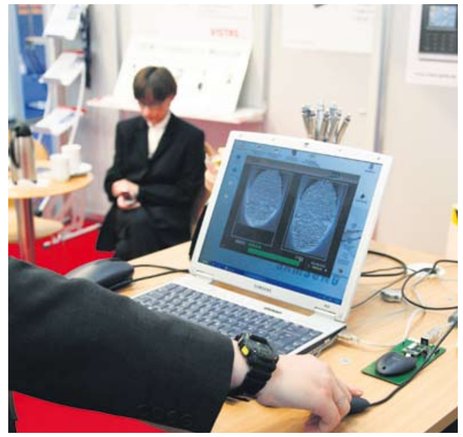
Die Basis für einen sicheren PC ist das Anti-Viren-Programm. Es sollte nicht nur auf jedem Rechner installiert sein, sondern auch stets aktuell gehalten werden. Schließlich kommen ständig neue Schadprogramme in Umlauf. Auch das Betriebssystem und der Internet-Browser müssen regelmäßig aktualisiert werden, die Hersteller bieten hierfür entsprechende Sicherheits-Updates an. Das Anti-Viren-Programm bietet allerdings keinen hundertprozentigen Schutz, deshalb sind zusätzliche Maßnahmen empfehlenswert. Zum Beispiel eine Firewall: Sie kontrolliert den Datenverkehr zwischen Computer und Internet. Wenn von außen versucht wird, auf den Rechner zuzugreifen, schlägt die Firewall Alarm. So verhindert sie Hackerangriffe oder einen Zugriff durch Schadsoftware. Anti-Spionage-Programme vervollständigen den Schutz: Sie funktionieren ähnlich wie ein Virenschutz, sind aber auf Spionage-Software spezialisiert.

Umsichtiges Verhalten ist ein weiterer Beitrag zum Schutz im Netz. Dadurch können vor allem Phishing-Versuche und Datenklau verhindert werden. So sollten persönliche Informationen nur ausgewählten Personen zur Verfügung gestellt werden, das gilt auch für soziale Netzwerke. Das Bezahlen beim Online-Einkauf oder Online-Banking sollte nur über eine gesicherte Internetverbindung – erkennbar am https vor der Webadresse – erfolgen. Auch halten richtig gewählte Passwörter Datendiebe fern. Sie sollten aus einer zufälligen Kombination von Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen bestehen. Eine Absicherung von Wechselmedien wie USB-Sticks ist ebenfalls ratsam. Der Symantec Internet Security Threat Report 2008 ergab, dass rund 65 Prozent der Schadprogramme über USB-Sticks und andere Wechselmedien von Rechner zu Rechner gelangt.

Beim elektronischen Briefverkehr gelten ebenfalls ein paar Vorsichtsmaßnahmen. Denn etwa zwei Drittel der E-Mail-Nutzer in Deutschland bekommen täglich mindestens eine unerwünschte Nachricht, jeder vierte sogar mehr als fünf Spam-Mails pro Tag. Spam ist nicht nur ein Ärgernis, sondern kann auch gefährlich werden. Schlimmstenfalls gelangen über Dateianhänge und Fotos Schadprogramme auf den Rechner. Die folgenden Grundregeln können einen Schaden verhindern: Nur E-Mails, deren Absender vertrauenswürdig ist, sollten überhaupt geöffnet werden. Falls der Absender unseriös erscheint: die Mail sofort löschen. Besondere Skepsis ist beim Öffnen von Anhängen oder Grafiken geboten. Spam-Filter helfen, die unerwünschte Post zu verringern – sie werden in der Regel schon beim E-Mail-Anbieter eingesetzt. Ergänzend dazu lassen sich weitere Filter auf dem eigenen PC installieren – entweder im E Mail-Programm oder als separate Software.

Biometrische Erkennung

CHRISTOPH BUSCH (Fraunhofer IGD / Hochschule Darmstadt, Teletrust)



Seit 2005 werden biometrische Daten in Reisepässen integriert. Das digitale Passbild erlaubt in Zukunft dem Grenzbeamten den visuellen Vergleich mit dem Passbesitzer und dient auch zur automatischen biometrischen Erkennung. Eine biometrische Gesichtserkennung ist am Frankfurter Flughafen für diesen Herbst geplant.

Unter Biometrie versteht man ein Verfahren zur Wiedererkennung von Personen. Biometrische Verfahren analysieren das Verhalten des Menschen (die Art- und Weise seines Tipverhaltens, die Merkmale seiner Unterschrift) oder die anatomischen Strukturen des Körpers (z.B. Gesicht, Iris, Fingerkuppe). Biometrische Systeme können als Verifikationssysteme oder als Identifikationssysteme ausgelegt sein. Bei einem Verifikationssystem gibt der Nutzer eine Identität vor, zu der im System eine Referenz vorliegt. Sofern biometrische Systeme mit einem authentischen Dokument kombiniert werden, kann das Referenzbild auf diesem Dokument abgelegt sein. Zum Zeitpunkt der Verifikation wird ein Vergleich mit genau diesem einen Referenzbild durchgeführt (1:1 Vergleich). Bei einem Identifikationssystem hingegen wird mit vielen eingelernten Bildern verglichen und aus dieser Menge das am besten passende Muster ermittelt (1:n Vergleich).

In der biometrischen Gesichtserkennung werden traditionell zweidimensionale Frontalbilder aufgenommen. Ein kritischer Faktor ist eine gute Bildqualität. Aus diesem Grunde wird darauf geachtet, dass wichtige Qualitätskriterien erfüllt sind. Dazu zählen guter Kontrast des 2D-Bildes, gleichmäßige Ausleuchtung und keine Verdeckung des Gesichtes durch Haare, Brillen oder Kopfbedeckungen.

Ein Hauptziel der aktuellen Forschung ist es, die Leistung der biometrischen Verfahren zu verbessern. Einer der Ansätze dabei ist es, multibiometrische Systeme zu entwickeln, die verschiedene biometrische Charakteristika in einer Aufnahme erfassen - beispielsweise das Gesichtsbild und die Geschichtsgeometrie [3dface2006]. Diese Informationen werden verknüpft und führen zu einer stabileren Aussage. Zudem wird durch gleichzeitige 3D-Gesichtserkennung eine verbesserte Robustheit hinsichtlich eines Überwindungsangriffes erreicht.

Eine relevante Frage bei der Nutzung eines biometrischen Systems ist die sichere und datenschutzfreundliche Speicherung. Biometrische Daten sind im Sinne der geltenden Datenschutzregelungen personenbezogene Daten und daher einem besonderen Schutz zu unterwerfen. Dies gilt besonders, wenn die Referenzdaten in einer zentralen Datenbank gespeichert werden, um eine kartenlose Komfort-Anwendungen zu realisieren. Mit der Speicherung in einer Datenbank werden einige potenzielle Probleme assoziiert: Diese reichen vom Identitätsdiebstahl bis zu dem Bedürfnis, gespeicherte Referenzdaten „zurückrufen“ zu können. Lösungsmöglichkeiten für diese Probleme werden entwickelt und sind in einem White-Paper Datenschutz in der Biometrie des TeleTrust-Verein publiziert.

Weitere Informationen

Die interdisziplinäre Diskussion über technische Machbarkeit und Datenschutzfreundliche Gestaltung von biometrischen Systemen wird in Deutschland im Wesentlichen in drei Fachverbänden geführt. Der TeleTrust-Vereins diskutiert Anwendungen und Datenschutz-Aspekte [ttt2009]. Die Fachgruppe BIOSIG der Gesellschaft für Informatik bietet eine Plattform für wissenschaftlichen Austausch [biosig2009]. Biometrische Standards werden entwickelt im Normenaussschuss des DIN [din2009].

Literatur: [3dface2006] 3D Face, http://www.3dface.org [biosig2009] BIOSIG, http://www.biosig.org [din2009] Normenausschuss NIA-37, http://www.nia.din.de [ttt2009]TeleTrust e.V., http://www.teletrust.org/fachgruppen/biometrie

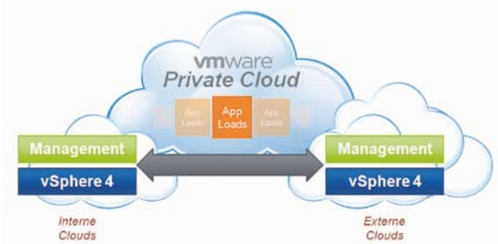
Die Freiheit liegt in den Wolken

VMware bildet mit seiner Virtualisierungstechnologie die Basis für Cloud Computing

Das Konzept ist simpel! So wie (die meisten) Unternehmen ihren Strom nicht selbst produzieren, nicht selbst als Telefonanbieter fungieren oder sich keine großen Gedanken darüber zu machen brauchen, dass ihr Leitungswasser auch trinkbar ist – so einfach kann auch die Nutzung von IT-Diensten sein. Das Konzept des Cloud Computing verlagert die Nutzung von IT-Diensten – in jeglicher Art und Konstellation – zu einem externen Dienstleister.

Unternehmen beziehen von extern ihre Rechenleistung je nach Bedarf – seien es Server, Speichersysteme oder spezielle Software. Die Anwendungen und Daten liegen somit nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern bei einem externen Anbieter. Gezahlt wird – wie beim Leitungswasser oder Strom – nur das, was man tatsächlich verbraucht. Cloud Computing bedeutet einen Paradigmenwechsel in der Art und Weise, wie IT bereitgestellt wird. Die unternehmenseigenen IT-Mitarbeiter werden von einigen Alltagssorgen – Ressourcenplanung, Administration, Speicherkapazität u.v.m. – entlastet.

Ohne Virtualisierung wäre das himmlische Cloud-Konzept nicht möglich. Die Technologie ermöglicht es, IT-Ressourcen flexibel zu gestalten, indem gewünschte Ergebnisse bzw. Dienste von den zugrunde liegenden physischen Ressourcen entkoppelt werden. Die Virtualisierung von Servern ermöglicht den Betrieb mehrerer Server auf einer physisch vorhandenen Maschine. Eine Virtualisierungslösung – die bekannteste ist die Virtualisierungsplattform ESX bzw. heute vSphere ™ 4 von VMware – ist zwischen die Hardware-Plattform und dem Betriebssystem angesiedelt. Sie gaukelt dem Betriebssystem vor, es wäre allein auf dem Server und könnte die gesamte Hardware für sich allein beanspruchen – während in Wirklichkeit mehrere (egal ob gleichartige oder unterschiedliche) Betriebssysteme auf dieser einen Maschine laufen. Durch diesen Kniff von der Hardware entkoppelt, also virtualisiert, können dann diverse Serverinstanzen, wie z.B. ein Datei- oder Webserver auf einer gemeinsamen Hardware-Basis friedlich koexistieren. Um die gerechte Verwaltung der tatsächlich vorhandenen Ressourcen kümmert sich ESX automatisch. Mit der im Frühjahr 2009 auf den Markt gekommenen, auf ESX-aufbauenden Lösung „VMware vSphere ™ 4“, hat VMware eine Plattform für die Cloud geschaffen, die große Teile der Infrastruktur zusammenfasst – Serverressourcen wie Prozessoren und Arbeitsspeicher – und sie ganzheitlich als nahtlose, flexible und dynamische Betriebsumgebung verwaltet. Auf VMware vSphere 4 läuft jedwede Applikation effizienter und mit garantierten Service-Leveln.



VMware im Höhenflug

Wie gut das funktioniert, zeigt, dass bereits in den ersten zwölf Wochen seit Erscheinen vSphere 4 350.000 Mal heruntergeladen wurde – das sind durchschnittlich 140 Downloads pro Stunde (!). 75 Prozent der VMware-Kunden wollen noch bis zum Jahresende 2009 von ESX 3.5 auf vSphere 4 upgraden.

VMware arbeitet eng mit branchenführenden ISVs zusammen, um eine möglichst breit angelegte Anwendungsunterstützung sicherzustellen und **branchenspezifische Anwendungen** – sei es für die Bereiche Finanzdienstleistung, Gesundheitswesen, Fertigung o.a. – anbieten zu können. Mehr als 1.200 VMware-Partnerunternehmen haben sich bereits zu der marktführenden Virtualisierungsplattform VMware vSphere™ 4 schulen lassen. Das im Jahr 2008 gestartete Service Provider Programm (VSPP) bietet den VMware-Partnern zusätzliche Schubkraft: VSPP ist Teil des VMware-Partner-Netzwerks und bietet zahlreiche Vorteile an, mit deren Hilfe Service Provider ihre VMware-basierten Dienste mit geringstmöglichen Overhead-Kosten anbieten können.

Offene Schnittstellen in den Wolken für mehr Flexibilität

Jedes Unternehmen kann sich dank Virtualisierung auch seine eigenen, internen Clouds aufbauen. Schließlich wird kaum ein Unternehmen alle IT-Services komplett auslagern, sondern immer nur gewisse Komponenten. Man unterscheidet hierbei zwischen internen und externen (von Drittanbietern genutzte IT-Dienste) Clouds. Durch Cloud Computing wird die IT-Abteilung vom „Verwalter“ zum Innovator und leistet einen wertvollen Beitrag zum Unternehmenserfolg: durch die Verbesserung bestehender Prozesse bis hin zur Schaffung der Basis für ganz neue Geschäftsmodelle.

Wer hat Angst vor Cybercrime?

ESET-Nutzer nicht!

ESET Smart Security 4

Antivirus | Antispyware | Firewall | Antispam

ESET NOD32 Antivirus 4

Antivirus | Antispyware

Die mehrfach ausgezeichneten Sicherheitslösungen von ESET bieten zu Hause, im Büro oder im Firmennetzwerk Schutz vor Viren, Spyware, Hackern, Spam und anderen Bedrohungen aus dem Internet – ohne Ihr System in seiner Performance und Geschwindigkeit zu beeinträchtigen. Schlagen Sie Cybercriminals die Tür vor der Nase zu!

Fragen Sie Ihren Fachhändler oder einfach downloaden unter **www.eset.de**