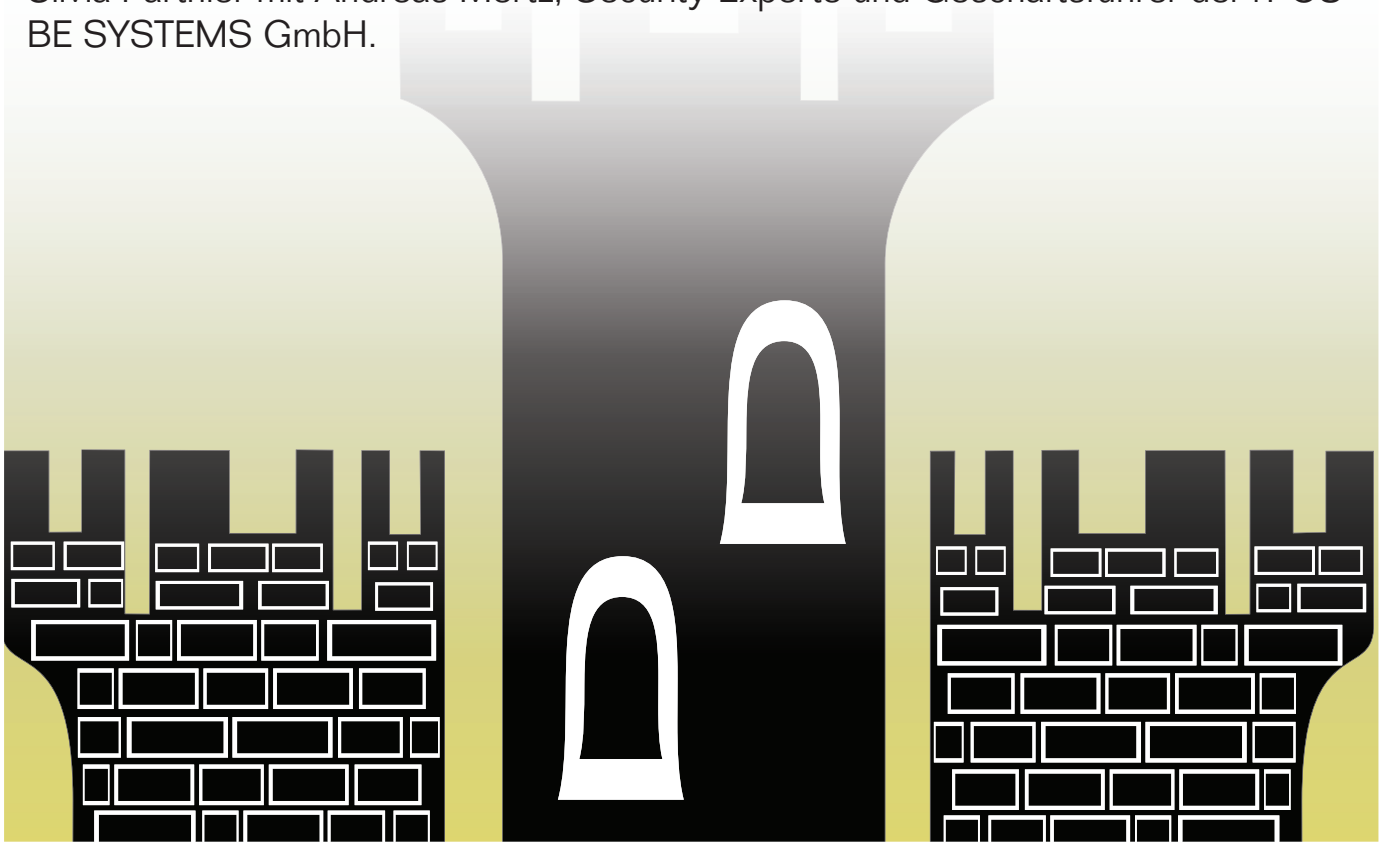
Paradigmenwechsel im Firewalling

Sieben Fragen zur aktuellen Firewall-Thematik

Der Markt der Firewalls ist hart umkämpft. Innovationen sind rar, dann aber bahnbrechend. Über den Wandel der Systeme und die Benefits für die Anwender sprach Silvia Parthier mit Andreas Mertz, Security-Experte und Geschäftsführer der iT-CUBE SYSTEMS GmbH.



? Extrem leistungsfähige Firewalls wie Checkpoint oder Cisco bedeuten auch einen hohen Administrationsaufwand. Sind diese Firewalls noch zeitgemäß?

Das hängt davon ab, wie Sie die Leistungsfähigkeit einer Firewall definieren. Der Begriff Firewall beinhaltet mittlerweile ein breites Spektrum von Sicherheitsfunktionen, wie Paketfilter, VPN, Proxies, IDS/IPS, etc. bis hin zu sogenannten Unified Threat Management Systemen (UTM). Zwar haben All-In-One-Systeme den Administrationsaufwand reduziert, jedoch nie wirklich Enterprise-Tauglichkeit erreicht. Wenn sich hinter einem funktionsgeladenen GUI ein Architekturmodell verbirgt, das lediglich den Verkehr durch verschiedene Filter-/Analysemodule hindurch schleift, stellt das leider keine echte Integration dar.

? Wo sehen Sie das Kernproblem?

Das Problem der meisten Lösungen, die im Kern noch immer auf Stateful

„Fair wäre, Wartungsgebühren nur noch für erkennbaren technologischen Fortschritt zu zahlen, statt für Bugfixes und kosmetische Änderungen. Fair wäre auch, Lizenzgebühren nur für Funktionen zu zahlen, die tatsächlich genutzt werden."
Andreas Mertz

Packet Inspection beruhen, ist deren zunehmender Verlust an Wirksamkeit. Weil ein User nicht mehr einer IP-Adresse und Applikationen TCP-/UDP-Ports nicht mehr fest zugeordnet werden können, greift der 15 Jahre alte Ansatz nicht mehr. Das Ziel der Erhaltung eines angemessenen Sicherheitsniveaus wird nicht mehr erreicht.

? Bei der Vielzahl von Produkten am Markt fällt der Überblick nicht leicht. Welches sind Ihrer Expertise nach derzeit wegweisende Firewalls?

Nachdem lange Zeit wenig Innovatives in der Perimeter Security zu sehen war, hat vor allem Palo Alto Networks im letzten Jahr unsere Aufmerksamkeit gewonnen.

? Aus welchem Grund?

Palo Alto Networks (PAN) hat Firewalling neu gedacht und konnte mit Merkmalen einer echten „Next Generation Firewall" aufwarten. Das System vereinigt sowohl bewährte Konzepte klassischer Lösungen als auch innovative Ansätze. HTTPS-Verkehr „on the fly" entschlüsseln, auf Angriffe und Malware scannen und gleichzeitig Applikationen erkennen, deren Verhalten interpretieren und diese ganz oder auf Funktionsebene filtern ist bahnbrechend. Basierend auf einer massiv-parallelen Prozessor-Architektur und einem flexiblen FPGA-Design markiert PAN gegenwärtig die technologische Spitze im Firewall-Segement. Das überzeugt auch immer mehr Kunden.

? Sehen Sie einen Trend hin zu „multifunktionalen Firewalls", also erweiterte Funktionen, die weit über das traditionelle Firewalling hinausgehen?

Bedenken wir die Veränderungen in der Applikationslandschaft, sind die erweiterten Kernfunktionen an ein solches System schnell definiert:

- Identifikation von Applikationen unabhängig von Port, Protokoll, Verschleierungsmethoden oder Verschlüsselung
- Identifikation von Benutzern unabhängig von der IP-Adresse
- Granulare Sicht und Kontrolle über Anwendungszugriffe und Funktionen
- Echtzeitschutz gegen in Anwendungen versteckte Bedrohungen
- Multi-Gigabit-Durchsatz, Inline Integration, minimale Latenzerhöhung

? Die hohen Lizenz- und Wartungsgebühren bei den Marktführern stören die Anwender enorm. Welches wäre ihrer Meinung nach ein faires Verfahren?

Fair wäre, Wartungsgebühren nur noch für erkennbaren technologischen Fortschritt zu zahlen, statt für Bugfixes und kosmetische Änderungen. Fair wäre auch, Lizenzgebühren nur für Funktionen zu zahlen, die tatsächlich genutzt werden. Und weil durchsatzstarke „Next Generation Firewalls" aufgrund der technischen Anforderungen spezifische Hardware-Appliances sein werden, sollte auch die Lizensierung auf Userbasis fallen. Auch hier hat Palo Alto Networks wegweisende Signale gesetzt.

? Als Systemintegrator steht bei Ihnen der Anwender im Fokus. Was raten Sie ihm aktuell hinsichtlich seiner Security-Infrastruktur?

Mit dem Einzug neuer Applikationen müssen IT-Security-Abteilungen ihre Sicherheitsarchitektur überdenken. Tun sie dies nicht, laufen sie Gefahr, den Fluss von Applikationen über Segmentgrenzen und Perimeter hinweg nicht mehr wirksam kontrollieren zu können. Wer also in den nächsten Monaten entscheiden muss, Firewall, Proxy, Content Scanner und/oder IPS zu erneuern, sollte kritisch hinterfragen, ob mit solchen Systemen jetzt und in den nächsten drei Jahren tatsächlich das angestrebte Sicherheitsniveau erzielt werden kann.

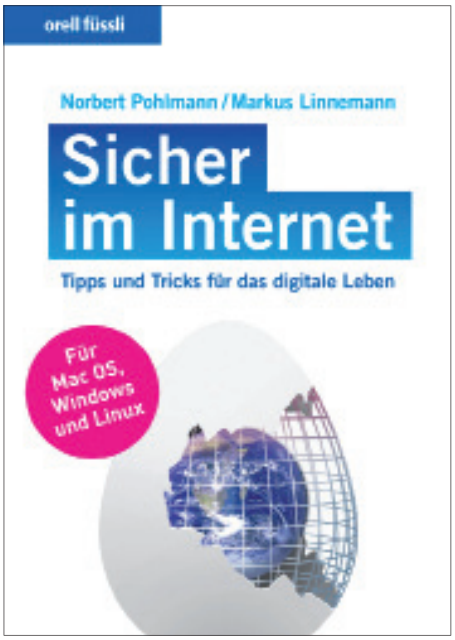
Herr Mertz, wir danken für das Gespräch!

Die Fragen stellte: *Silvia Parthier*

Es antwortete: *Andreas Mertz*

Sicher im Internet

Tipps und Tricks für das digitale Leben



Updates, Passwörter, Verschlüsselung, Kindersicherung: Irgendwie weiß jeder Computerbenutzer, dass ihn das etwas angeht. Dass er Bescheid wissen müsste. Um sicher zu sein im Internet. Die wenigsten haben jedoch den Durchblick oder gerade einen IT-Crack zur Hand. Und doch müssen sie ihre Daten sichern.

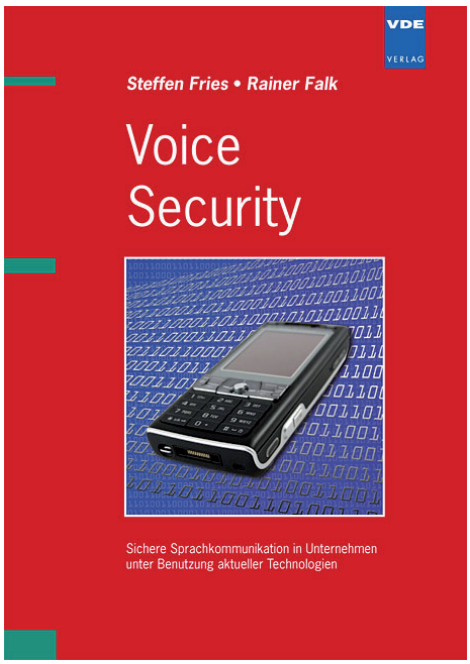
Norbert Pohlmann und Markus Linnemann, zwei anerkannte Experten für Internet-Sicherheit, ersetzen den Fachmann in jedem Computerhaushalt. Schritt für Schritt erhellen sie den Weg durch den gefährlichen Dschungel der IT-Welt. Einfach und verständlich, mit Checklisten, Tipps und einem speziellen Online-Service mit aktualisierten Informationen. Das spart Geld und macht sicher.

Norbert Pohlmann /
Markus Linnemann

Sicher im Internet
Tipps und Tricks für das digitale Leben
Orell Füssli Verlag, Zürich 2010
192 Seiten, broschiert
ISBN 978-3-280-05375-1
Fr. 34.90 / € 19.90

Voice Security

Sichere Sprachkommunikation in Unternehmen unter Benutzung aktueller Technologien



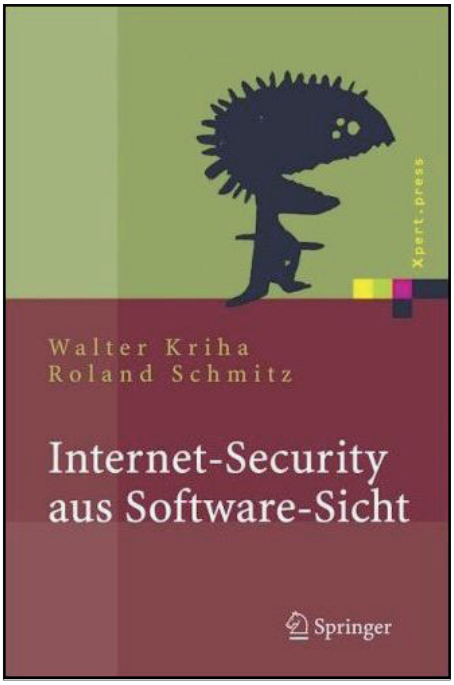
Sprache ist neben der heute gängigen Kommunikation via E-Mail die in Geschäftsprozessen am meisten verwendete Technologie für die Kommunikation. Da die Kommunikation oftmals sensible oder firmenkritische Themen beinhaltet, ist ein angemessener Schutz der kommunizierten Inhalte von großer Bedeutung.

Historisch gesehen waren Sicherheitsmaßnahmen bei Sprachdiensten meist gegen Gebührenbetrug gerichtet, sie dienten im Wesentlichen also dem Schutz des Betreibermodells. Andere Ansätze kamen eher aus dem militärischen Bereich, um Kommunikation in einem Ende-zu-Ende-Ansatz vor Abhören zu sichern. Keine der beiden Zielsetzungen zieht jedoch die Sicherheitsanforderungen für sensitive Unternehmenskommunikation unter Berücksichtigung von privaten und öffentlichen Kommunikationswegen direkt in Betracht.

Dieses Buch verfolgt einen anderen Ansatz: Nach einer Einführung in aktuelle Sprachtechnologien wird die Sicherheit dieser Technologien beschrieben und analysiert. Der Fokus liegt dabei auf Voice over IP (VoIP) unter Einbeziehung von Festnetz- und Mobilkommunikation mittels GSM, UMTS und WiMAX. Die erreichten Sicherheitseigenschaften und mögliche Einschränkungen dieser Ansätze bilden die Basis für das Verständnis der entsprechenden Risiken in der Unternehmenskommunikation. Ein in Bezug auf Sicherheitsanforderungen funktional angepasster Ansatz ermöglicht die schrittweise Einführung von Sicherheitsfunktionen für Sprachdatenkommunikation, entsprechend den Sicherheitsstufen, die aus der Datenkommunikation bekannt sind: vertraulich, streng vertraulich etc.

172 Seiten, DIN A5, 40,-., VDE Verlag,
ISBN 978-3-8007-3078-0

Internet Security aus Software-Sicht



Dies ist der erste Band in der Reihe Internet-Security. Er beschäftigt sich in erster Linie mit Grundlagen sicherer Software und versucht anhand von Beispielen und Fallstudien ein Verständnis für die Sicherheitsproblematik in schaffen.

Das Buch beginnt mit einer eher geschäftlichen Sicht auf die Sicherheit von Portalen. Anschliessend wird gezeigt wie Sicherheitsanalysen erstellt werden können. Im Anschluss daran werden Grundlagen wie die Sicherheit in verteilten Systemen und Middleware besprochen sowie Basistechniken und Protokolle vorgestellt.

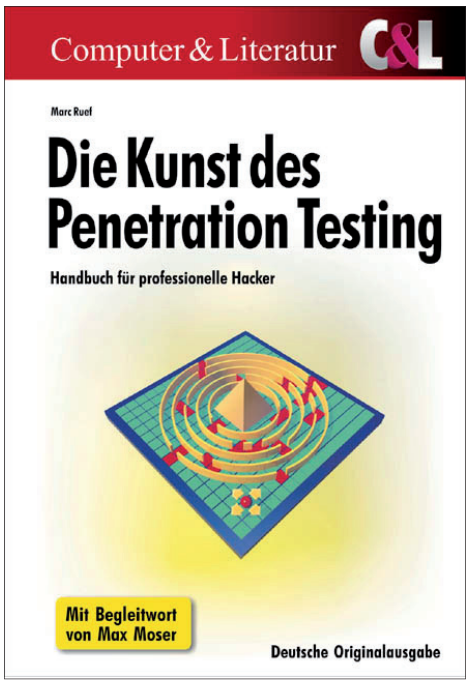
Kapitel zu Sicherheitsfragen bei Content-Management Systemen, der Aufbau einer DMZ unter Berücksichtigung der Auswirkungen auf die Softwarearchitektur und eine Diskussion föderativer Sicherheit schließen den Band ab.

Verglichen mit dem 2. Band: Sichere Systeme, hat der erste Band eher mit der klassischen Sicht auf sichere Software zu tun: Sie hat die rechtliche oder geschäftliche Sicht durchzusetzen und verwendet dazu Techniken wie Authentisierung und Autorisierung. Es werden die Grenzen Kanalbasierter Sicherheit klar aufgezeigt. Wichtig ist uns, dass Entwickler zunächst überhaupt die Wahrnehmung von Sicherheitsproblemen schärfen können und dabei einige grundlegende Techniken und ihre Anwendung lernen.

Der zweite Band mit dem Titel „Sichere Systeme“ geht einen grundsätzlich anderen Weg und betont viel stärker den kausalen Aspekt von sicherer Software: sie muss nicht nur korrekte Geschäftsprozesse erlauben sondern auch kalkulierbar in ihren Aktionen sein. Sprich den „Safety“ Aspekt von Systemen ebenfalls abdecken. So stellen etwa. Buffer Overflows keine Verletzung der rechtlichen Regeln dar innerhalb eines Web Services. Stattdessen hebeln die die ganze Plattform aus

W. Kriha, R. Schmitz: Internet Security aus Software-Sicht Springer 2008. Etwa 300 S., Geb.
ISBN: 978-3-540-22223-1

Die Kunst des Penetration Testing



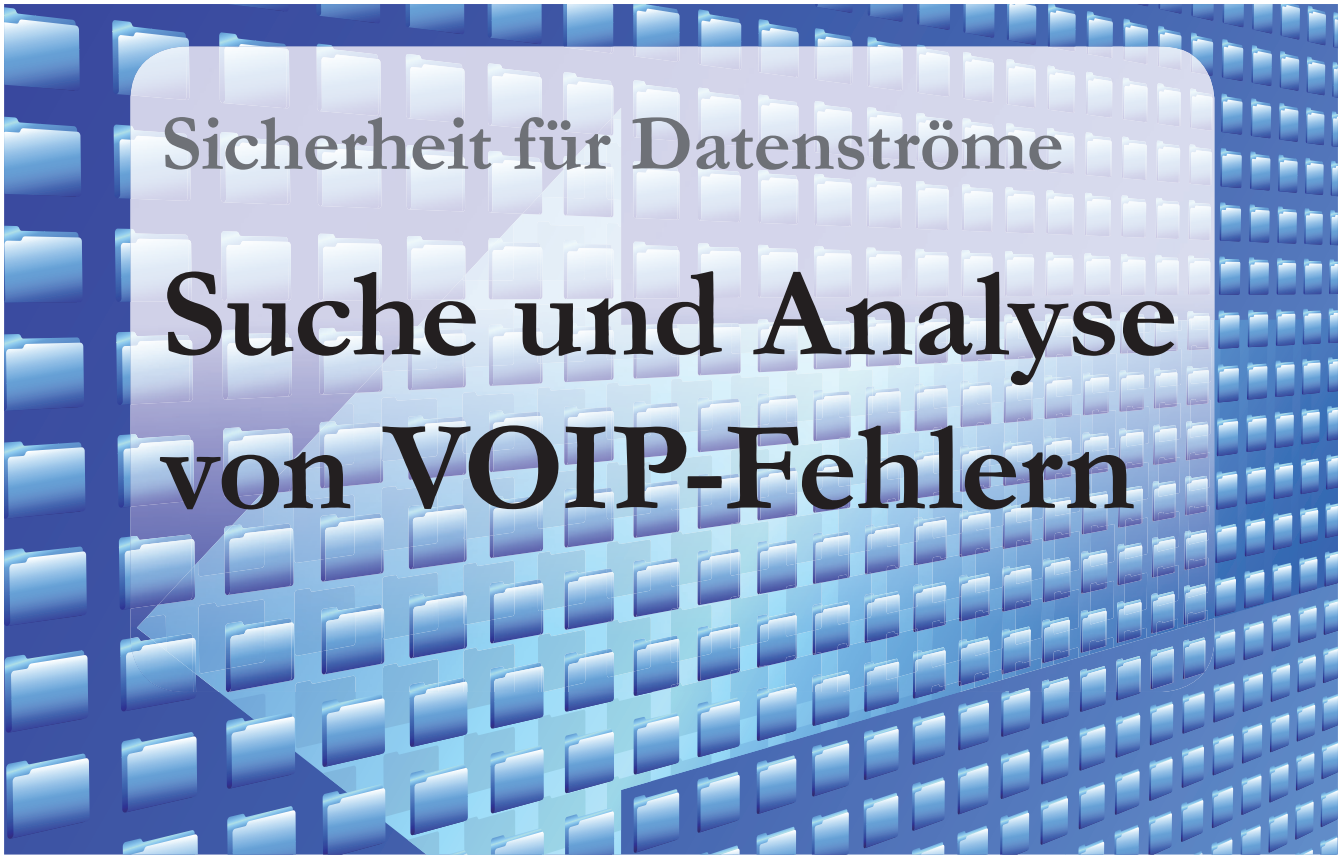
Kein funktionsfähiges Unternehmensnetzwerk kann so abgeschottet werden, dass es hundertprozentige Sicherheit bietet. Gern wird übersehen, daß es aber nicht nur von außen erreichbar ist, auch durch Mitarbeiter sind ungewollte Zugriffe möglich. Es ist deshalb unabdingbar, Netzwerk und Anwendungen in regelmäßigen Abständen anhand simulierter Angriffe auf bekannte und unbekannte Sicherheitslücken zu untersuchen.

Dieses Buch ist ein systematischer Leitfaden für solche Penetration-Tests und richtet sich an Security Consultants, die sich in die Materie einarbeiten müssen oder Kenntnisse vertiefen wollen. Einleitend klärt es die administrativen Voraussetzungen für ein professionelles Vorgehen vor Ort. Die ausführlichen Kapitel zu

- Footprinting
- Mapping und Application Mapping
- Portscanning
- OS- und Application Fingerprinting
- Denial of Service

liefern detaillierte technische Anleitungen für die kontrollierte Durchführung von Angriffen. Dabei wird auch beschrieben, wie Firewalls umgangen werden und welche Schwachstellen mit Exploits ausgenutzt werden können.

Marc Ruef : Die Kunst des Penetration Testing C&L Computer- und Literaturverlag GmbH
ISBN-13 978-3-936546-49-1,
911 Seiten, 49,90



Sicherheit für Datenströme

Suche und Analyse von VOIP-Fehlern

Die Telefon- und Datenkommunikation ist im heutigen geschäftlichen Umfeld als Kommunikationsmittel wichtiger denn je. Immer mehr Applikationen aus der Telefon-, Video- und Datenwelt sind bereits oder werden in Zukunft untrennbar im so genannten Unified Communications (UC) miteinander verknüpft.

Die Bereitstellung von Sprachanwendungen (VoIP) erfordert die Anpassung der Netzwerke an die erhöhten Anforderungen der Echtzeitanwendungen. Die Integration von Daten, Sprach- und Videoanwendungen benötigt die Bereitstellung einer garantierten Bandbreite als Grundlage der applikationsspezifischen Merkmale auf einer Ende-zu-Ende-Basis (von Endgerät zu Endgerät). Der Einsatz von Echtzeitanwendungen erfordert jedoch ein barrierefreies Zusammenspiel zwischen den Anwendungen und den Transportkanälen.
Echtzeitapplikationen wie VoIP erfordern einen tadellosen Betrieb der Netzwerkkomponenten. Kleinste Fehler in der Netzwerkkonfiguration können bei VoIP zu hörbaren Fehlern mutieren.

Durch Vormessungen lassen sich Netzwerke auf ihre VoIP-Fähigkeit überprüfen. So können Fehler im Netzwerk bereits vor der Implementation von VoIP gefunden und beseitigt werden. Nach der VoIP-Installation lassen sich die Qualitäten der VoIP-Gespräche dauerhaft überwachen, so dass Änderungen der Sprachqualität sofort entdeckt werden. Eine Überwachung der Sprachströme ist empfehlenswert, da sich Netzwerke in der Praxis kontinuierlich verändern. Jede Änderung im Netzwerk kann zu Einbußen der VoIP-Qualität führen. Durch die kontinuierliche Netzüberwachung wird jede VoIP-Änderung erkannt und das Messsystem generiert automatische Alarme, so dass der VoIP-Techniker rechtzeitig eingreifen kann, bevor diese sich beim Nutzer negativ auswirken. Neue softwarebasierenden Messtechniklösungen im Bereich Triple-Play-Messtechnik bieten Sicherheit und eignen sich hervorragend zur Fehlersuche und das Testen von VoIP-Netzwerken.

Sprachqualität bei VoIP

Bei VoIP werden die Gespräche in IP-Pakete verpackt und über die IP-Infrastruktur verschickt. Die „Sprache“ muss sich bei VoIP die physikalischen Übertragungsressourcen mit anderen Applikationen teilen. Um einen einwandfreien Betrieb zu garantieren, müssen einige Vorkehrungen getroffen werden. Hierzu sind folgende Aspekte zu beachten:

- Sprachqualität: Die Sprachqualität beschreibt, wie gut die Verständlichkeit einer menschlichen Stimme bei Aufzeichnung und Wiedergabe durch die technischen Einrichtungen (Endgeräte, Netzwerkkomponenten, Gateways) sind. Die Bewertungskriterien der Sprachqualität sind durch die ITU-Bewertungsmethoden im Standard P.800 spezifiziert. Das bekannteste Sprachbewertungsverfahren ist der so genannte „Mean Opinion Score“ (MOS). Mit Hilfe des MOS werden die Übertragungsqualitäten unterschiedlicher Sprachströme und Codierungen miteinander verglichen. Der MOS-Wert wird subjektiv ermittelt, indem Sprechproben den Probanden vorgespielt, die einzelnen Bewertungen gewichtet und daraus die statistischen Ergebnisse ermittelt werden. Beim MOS handelt es sich um einen Wert zwischen eins und fünf, der für die Sprachqualität steht; wobei der Wert »1« eine mangelhafte Sprachqualität repräsentiert, bei der keine Verständigung möglich ist, der Wert »5« hingegen für eine exzellente Übertragungsqualität steht, die nicht von dem Original zu unterscheiden ist.

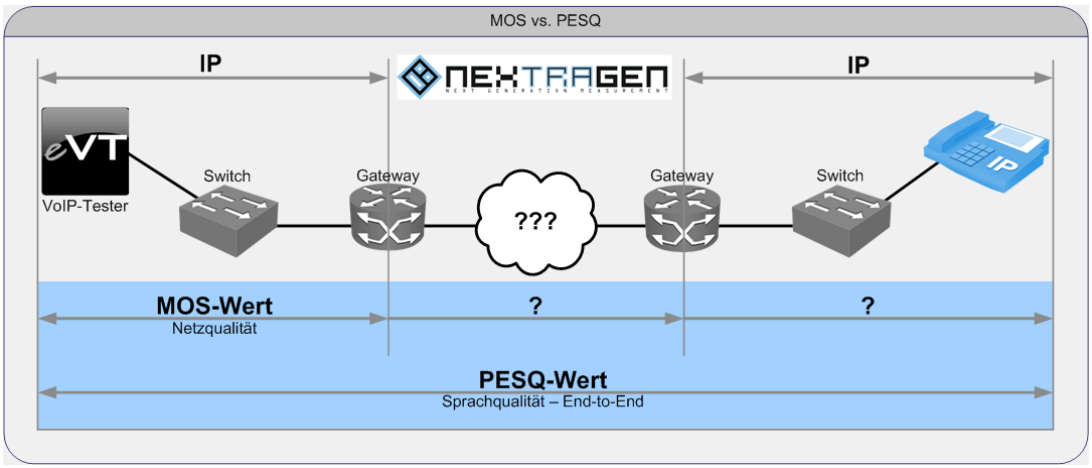


Bild 1: Der PESQ-Algorithmus spezifiziert ein aktives Berechnungsmodell zur Bestimmung der Sprachqualität und basiert auf den realen Bedingungen einer Ende-zu-Ende-Sprachkommunikation. Das Verfahren berücksichtigt unter anderem Paketverluste, Rauschen und den verwendeten Sprachcodec.

Die ITU-T-Empfehlung G.107 beschreibt mit dem E-Modell ein Berechnungsmodell zur Bestimmung von objektiven Qualitätsparametern für Sprachverbindungen. Das E-Modell ist ein passives Modell zur Bestimmung der Sprachqualität. Das Messsystem berechnet aus einem übermittelten VoIP-Strom, die für das E-Modell notwendigen Parameter. Nach der Übergabe der Parameter an das E-Modell gibt das Messsystem einen Übertragungsfaktor (R-Faktor) aus. Aus diesen Werten wird eine Vorhersage der Sprachqualität im Bereich 0 bis 100 getroffen, die auf der MOS-Skala abbildbar ist. Der PESQ-Algorithmus spezifiziert in der ITU Vorschrift P.862 ein aktives Berechnungsmodell zur Bestimmung der Sprachqualität und basiert auf den realen Bedingungen einer Ende-zu-Ende-Sprachkommunikation.
Das Verfahren berücksichtigt unter anderem Paketverluste, Rauschen und den verwendeten Sprachcodec. Bei der PESQ-Analyse wird ein Referenzsignal und das durch die Übermittlung über das Netzwerk geminderte Signal in das System eingegeben. Bei diesem Modell wird das Sprachsignal zur Beurteilung hinzugezogen. Dabei werden alle Fehler sichtbar, auch diese, die außerhalb des IP-Netzwerks liegen.

- Verzögerung: Die Verzögerung beschreibt die Latenzzeit zwischen dem Auftreten eines Ereignisses und dem Auftreten eines erwarteten Folgeereignisses, um das ein Ereignis verzögert wird. In Netzwerken wird die Verzögerung oft mit dem Begriff Round Trip Time (RTT) beschrieben. Der Round Trip Delay beschreibt die Gesamtverzögerung (Hin- und Rückweg) zwischen zwei IP-Endpunkten. Bei VoIP-Anwendungen und Videokonferenzen ist das so genannte One Way Delay (die Verzögerung in einer Richtung) von Bedeutung. Netzwerkverzögerungen werden durch die physische Verzögerung der Übertragungsleitungen, der Queuing- und Pufferungsmechanismen in den Koppelkomponenten (Router, Switches, Gateways) verursacht und variieren in ihrem Ausmaß. Die Spezifikation gemäß G.114 der ITU-T erlaubt eine Ende-zu-Ende-Verzögerung von maximal 150 ms. Alle darüber hinausgehenden Verzögerungswerte verschlechtern die Sprachqualität.

- Paketverluste: Die Paketverlustrate definiert, wie viele Pakete eines Datenstroms zwischen einem Sender und einem oder mehreren Empfängern während der Übertragung verloren gegangen sind. Für eine qualitativ hochwertige Verbindung sollte dieser Fehlerwert so klein wie möglich sein. Optimal aus-

gelegte und gut administrierte IP-Backbones weisen heute in

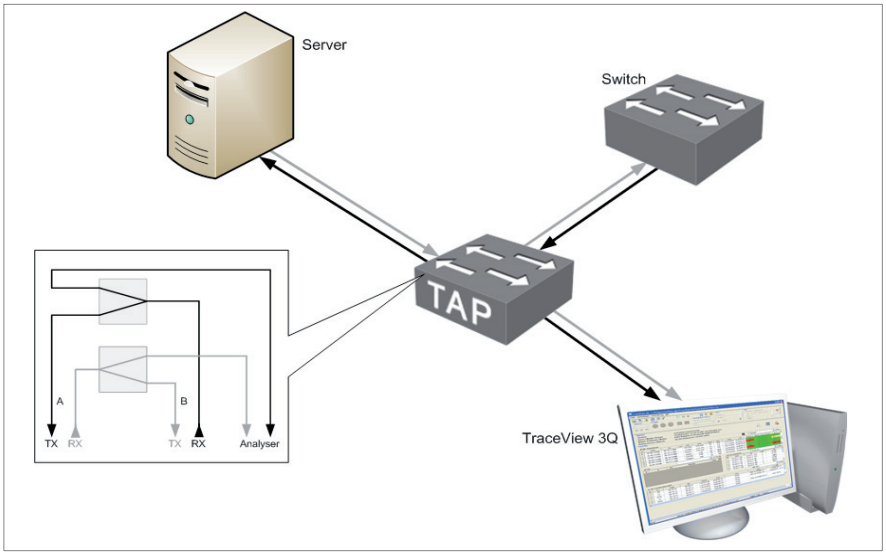


Bild 2: Bandbreitenengpässe sind ein mögliches Störpotenzial beim Einsatz der VOIP-Technik.

der Regel eine Paketverlustrate von < 0,5 Prozent auf. Für die Übermittlung von VoIP-Datenströmen gilt eine Paketverlustrate bis zu 5 Prozent als noch akzeptable Qualität. Paketverluste wirken sich umso stärker aus, je länger der so genannte Payload (Sprach/Videoanteil im Paket) ist. Codecs weisen eine gewisse Toleranz gegenüber Paketverlusten auf. In Abhängigkeit vom genutzten Codec der Anwendung bemerkt der Nutzer die unterschiedlich stark aufgetretenen Paketverluste nicht.

- Jitter: Als Jitter bezeichnet man allgemein ein Taktzittern bei der Übertragung von Digitalsignalen bzw. eine leichte Genauigkeitsschwankung im Übertragungstakt. In der Netzwerktechnik wird mit Jitter außerdem die Varianz der Laufzeit von Datenpaketen bezeichnet. Dieser Effekt ist insbesondere bei interaktiven Multimedia-Anwendungen störend, da dadurch Pakete zu spät eintreffen können, um noch zeitgerecht mit

ausgegeben werden zu können. Im Idealfall sollte der Jitter bei 0 ms liegen, dies ist in heutigen Netzwerken nicht möglich. Daher muss dieser Parameter kontrolliert werden. Diese Parameter sind entscheidende Faktoren für den problemfreien Betrieb von VoIP.

Aktive Überwachung

Mit Hilfe des Trafficlyser TraceSim VoIP können vor Inbetriebnahme die Netze durch eine Simulation von Gesprächen geprüft werden. Hier kommt der PESQ-Algorithmus zum Einsatz, welcher eine Aussage über die Ende-zu-Ende Qualität liefert. Nach einem empfohlenen Messzyklus von einer Woche für eine VoIP-Vormessung kann eine Aussage getroffen werden, ob ein Netzwerk „VoIP-Ready“ ist. Bei den Messungen werden zwischen zwei oder mehreren IP-Endpunkten realistische Telefonverhalten aktiv nachgebildet und das Netzwerk wird mit echten Telefongesprächen getestet.

Nach der Vormessung kann das System auch weiterhin als aktive Langzeitüberwachung eingesetzt werden, welche dauerhaft Gespräche simuliert und automatisch alarmiert, wenn die Qualitäten einstellbare Schwellwerte unterschreiten.

Passive Überwachung

Durch den Einsatz einer passiven Monitorlösung lassen sich laufende Gespräche überwachen. Hier können ebenfalls Schwellwerte voreingestellt werden, wann alarmiert werden soll. So wird die Qualität auch während des Betriebes kontrolliert. Durch die Monitoring-Lösung werden die eigentlichen Gesprächsdaten nicht angefasst, so ist ein „Abhören der Gespräche“ nicht möglich. Eine Verschlüsselung der Gesprächsdaten (beispielsweise mit dem Securc RTP-Protokoll) erhöht in der Praxis die Sicherheit der Datenströme. Dadurch kann ein Dritter die Sprachströme mit Hilfe eines Analysators zwar aufzeichnen, die eigentlichen Sprachdaten lassen sich Aufgrund der Verschlüsselung jedoch nicht darstellen. Die Nutzung der verschlüsselten Übermittlung der Sprachdaten beeinflusst nicht die VoIP-Messungen. Sprachqualität und Sicherheit sind also kein Gegensatz, sondern ergänzen sich hervorragend.

Benjamin Kolbe
CTO, Nextragen GmbH

„Nach der VoIP-Installation lassen sich die Qualitäten der VoIP-Gespräche dauerhaft überwachen, so dass Änderungen der Sprachqualität sofort entdeckt werden. Eine Überwachung der Sprachströme ist empfehlenswert, da sich Netzwerke in der Praxis kontinuierlich verändern.“
Benjamin Kolbe
CTO Nextragen GmbH

Quarantäne-Station für infizierte Mails

Der Netzwerksicherheitsspezialist WatchGuard Technologies präsen-tiert mit dem Quarantine Management Server (QMS) eine neue Qua-rantäne-Lösung für E-Mail-Gateways.

Diese verleiht den Produkten der Watch-Guard XCS-Familie (Extensible Content Security) erweiterte Schutzfunktionen gegenüber Spam, Phishing und Malware. Die jüngste Entwicklung des Security-Experten ermöglicht es mittelgroßen und großen Unternehmen, unerwünschte E-Mails und Mittei-lungen mit besonders umfangreichen Datenmengen zur weiteren Verarbeitung und Überprüfung an einen lokalen Quarantäne-Server umzuleiten. Durch diesen zusätzlichen Sicherheitsbereich ergibt sich ein umfassender Schutz vor Bedrohungen. Darüber hinaus erhalten auch die Administratoren ein Höchstmaß an Flexibilität und Kontrolle.

Als geschäftskritische Anwendung ist der E-Mail-Verkehr besonders häufig Angriffspunkt für Viren, Hacker und Malware. Mit dem neuen Produkt er-gänzt das Unternehmen seine XCS-Reihe zielgerichtet im Bereich des Mes-saging und der Content Security. Unternehmen, die ihre XCS-Produkte mit dem QMS kombinieren, erhalten vollständige Kontrolle über Mitteilungen und höchstmöglichen Schutz vor bösartigen E-Mails. Zudem sinken mit der neuen Lösung die Anforderungen an Speicherkapazitäten von bestehenden E-Mail Security Gateways, was zu einem höheren Datendurchsatz beim E-Mail-Versand führt. Gleichzeitig können die Anwender Administrationsko-sten reduzieren. Auch das Reporting läuft optimierter ab. Der WatchGuard QMS speichert und verwaltet Spam-Mails für bis zu 180.000 Nutzer und sichert die jeweiligen Mitteilungen für 30 Tage und mehr. So wird garan-tiert, dass seriöse Nachrichten nicht verloren gehen und Speicher- sowie Bandbreitenanforderungen eingehalten werden können.

Bild 1: QMS 500

Bild 1: QMS 1000

Impressum

Chefredakteur:
Ulrich Parthier

Redaktion:
Silvia Parthier

Autoren dieser Ausgabe:
Werner Blessing, Steffen Gundel, Prof. Dr. Thorsten Holz, Wolfgang Hustädt, Benjamin Kolbe, Achim Kraus, Florenz Lammert, Prof. Dr. Ing. Clemens Martin, Andreas Mertz, Ulrich Parthier, Silvia Parthier, Markus Stratmann

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Rudolf-Diesel-Ring 32, D-82054 Sauerlach
Tel.: +49 8104 6494-0
Fax.: +49 8104 6494-22
www.it-verlag.de

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
100% des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Alle Autoren erreichen Sie über die Redaktion.
Wir reichen Ihre Anfrage gerne an die Autoren weiter.
Manuskripteinsendungen: Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signaturen des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung: Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung, Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigungen eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout & Satz:
Sabrina Hein

Druck:
Gebr. Geiselberger Druck
www.geiselberger.de

Objektleitung:
Ulrich Parthier (-14)

ISSN-Nr.: 1438-5503
Erscheinungsweise: zweimonatlich

Verkaufspreis:
Einzelheft € 20,- (Inland)
Jahresabonnement € 100,- (Inland) bzw. € 110,- (Österreich, Schweiz) bei Zustellung per Normalpost.

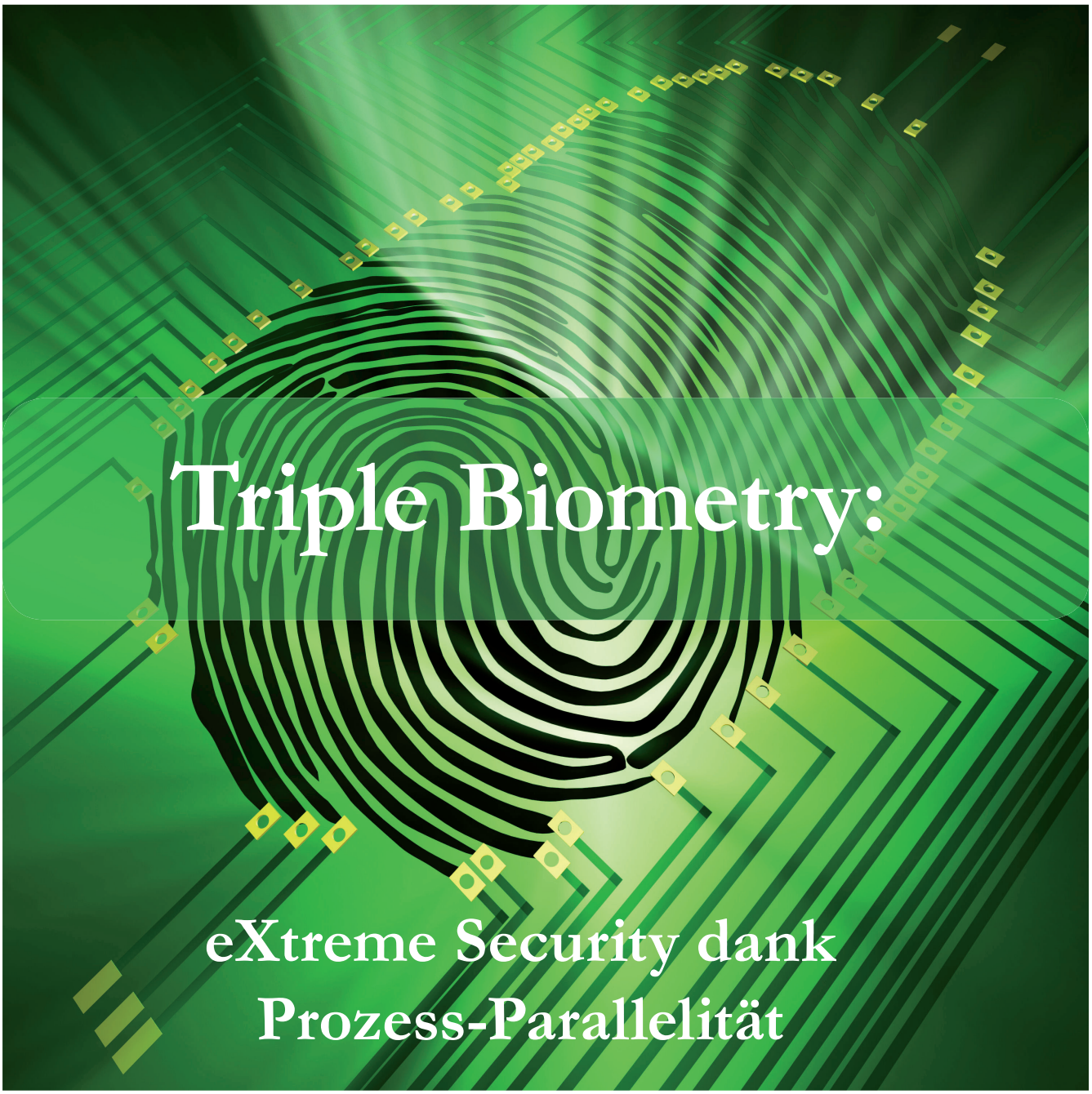
Bankverbindung:
VRB München Land eG,
BLZ 701 664 86, Kontonummer 25-23752

Abonnementservice:
Das Abbonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Bezugsgelder.

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 10
gültig ab Januar 2010

Anzeigenverkauf:
Deutschland:
Carmen Keller- Maiwald
Rudolf-Diesel-Ring 32
82054 Sauerlach
Tel.: +49 8392 / 93 42 42
Fax: +49 8392 / 93 42 43
E-Mail: keller-maiwald@it-verlag.de

USA:
Global Ad-Net
Mr. Ed Ware
80 Elm Street, Suite 2, Peterborough, NH 03458
Phone: 603-924-1040
Fax: 603-924-1041
E-Mail: ed@globalad-net.com



Triple Biometry:

eXtreme Security dank Prozess-Parallelität

Biometrie hält immer mehr Einzug in unserem Leben. Sei es durch den biometrischen Pass, Fingerprint am Laptop, Handvenenscanner, Kontrolle des Tippverhaltens oder Stimm- und Gesichtskontrollen bei Zutritt zu gesicherten Gebäuden.

Das Angebot zur Absicherung des Computers und der vertraulichen Daten ist groß. Viele Hersteller setzen dabei auf ein einzelnes biometrisches Verfahren, wie etwa die in den meisten Laptops eingebauten Fingerprints oder Smartcards. Doch auch diese Systeme sind teilweise sehr leicht fälschbar. Was liegt also näher als mehrere Verfahren miteinander zu kombinieren. Bereits bei der Kombination von zwei Methoden sprechen wir von Strong Authentification.

Die Biometry.com AG aus der Schweiz hat eine Softwarelösung entwickelt, die drei biometrische Verfahren gleichzeitig abfragt. Dadurch wird ein Identitätsbetrug nahezu unmöglich. Die Software BIOMETRYsso arbeitet mit der Stimm-, Gesichts- und der Worterkennung. Bei der Authentisierung laufen 12 Prozesse gleichzeitig ab, was höchste

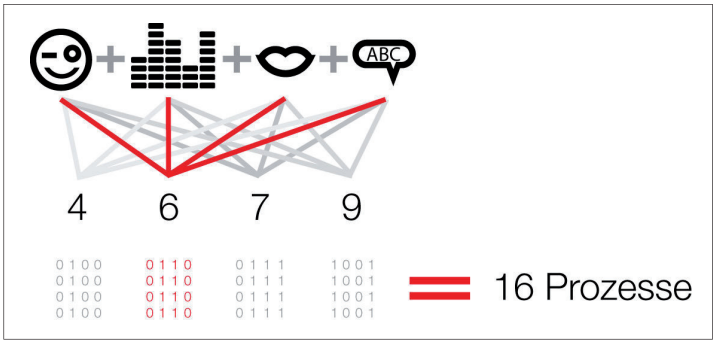


Bild 1: Parallele Prozessabfragen sorgen für ein hohes Sicherheitsniveau.

Sicherheit gewährleistet. Nutzer können damit ihre passwortgeschützten Dateien, Programme auf dem Computer sowie Internetanwendungen absichern. ComBiom, die technologische Basis der Lösung wurde von dem Institut geprüft, das auch die Software für den deutschen biometrischen Pass verifiziert hat. Das Ergebnis zeigt, dass der EER von ComBiom eine glatte Null ergibt; FRR und FAR gehen getrennt in die Nulllinie (s. Interview im Kasten). Hintergrund ist die extreme Anfälligkeit von Passwörter als Schutzmaßnahme. Auch Policies in den Unternehmen, die in bestimmten Zeiträumen neue Paßwörter zwingend vorschreiben, helfen nur begrenzt weiter. Lediglich alpha-numerische Passwörter mit Sonderzeichen und acht Stellen aufwärts bieten eine gewisse Sicherheit und sind schwierig zu knacken. Die Frage nach Alternativen, die nicht das Erinnerungsvermögen der Mitarbeiter strapaziert, ist also durchaus berechtigt.

Bei BIOMETRYsso funktioniert das wie folgt: Wenn der Benutzer eine passwortgeschützte Datei oder Anwendung öffnen möchte, erscheint ein Webcam-Blickfeld und er wird aufgefordert die nacheinander auftauchenden Ziffern nachzusprechen. Mit der Webcam und dem Mikrofon werden sein Gesicht und seine Stimme aufgezeichnet. BIOMETRYsso prüft nun, ob die Aufzeichnungen mit den vorab gespeicherten Templates übereinstimmen. Wenn ja, wird die Anwendung geöffnet. Ein Vorteil für den Nutzer ist dabei: BIOMETRYsso ist eine Single-Sign-On-Lösung. Das heißt, ist der Nutzer einmal authorisiert, kann er auch alle anderen passwortgeschützten Programme öffnen ohne sich noch einmal anmelden zu müssen.

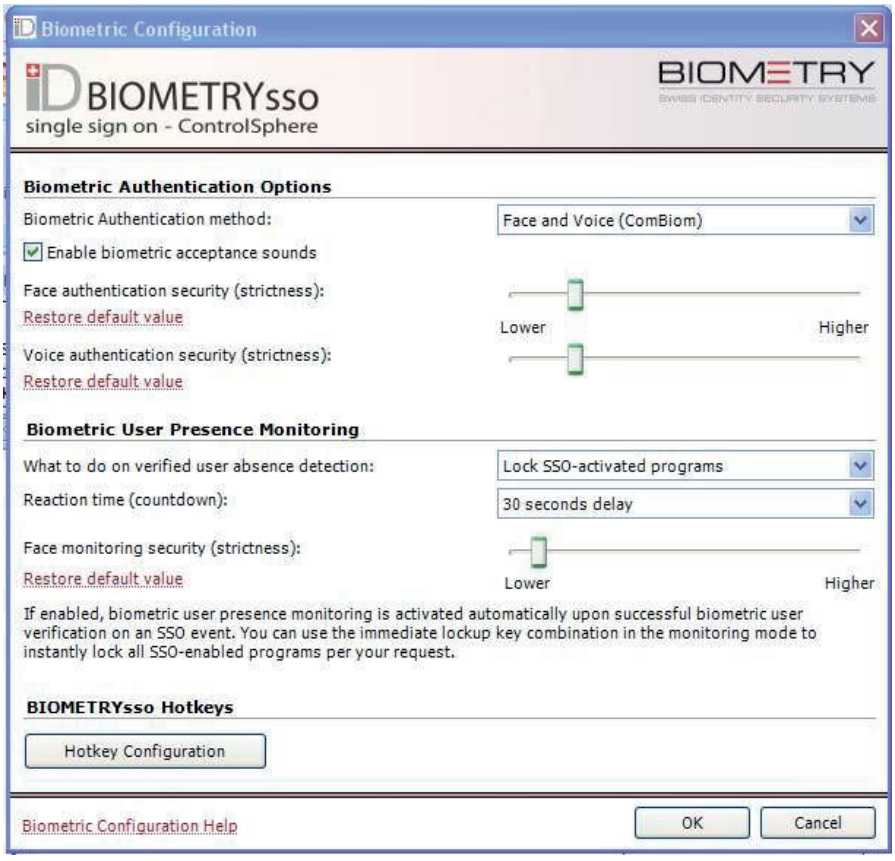


Bild 2: Einstellungen der Optionen bei BIOMETRYsso.

Dadurch dass gleich drei biometrische Verfahren simultan benutzt werden, ist die Lösung wesentlich sicherer als andere Produkte. Das Gesicht, die Stimme und die Worterkennung gleichzeitig zu fälschen, ist so gut wie unmöglich. Die meisten Hersteller setzen aktuell auf ein biometrisches Verfahren oder die biometrischen Verfahren werden nacheinander abgefragt. Das ist weitaus einfacher zu fälschen.

Beispiele

In vielen Laptops sind heutzutage Fingerabdruckleser eingebaut. Beim Desktop-PC wird oftmals ein separates Lesegerät angeschlossen. Die „Fingerprints» sollen das Passwort durch ein angeblich sicheres biometrisches Verfahren ersetzen. Wollen Angreifer den PC knacken, brauchen sie lediglich den Fingerabdruck des Besitzers. Dieser kann beispielsweise von einem Gegenstand mit ein paar Hilfsmitteln abgenommen und auf den eigenen Finger übertragen werden. Die Systeme fallen leicht auf Täuschungsversuche herein.

Wenn Angreifern versuchen, sich über das Netz Zugriff zum Computer zu verschaffen, werden automatisch alle Anwendungen geschlossen, so dass der Versuch scheitert. Möchte der PC- oder Laptop-Benutzer während der gesamten Zeit in der das Gerät an ist, eine Absicherung

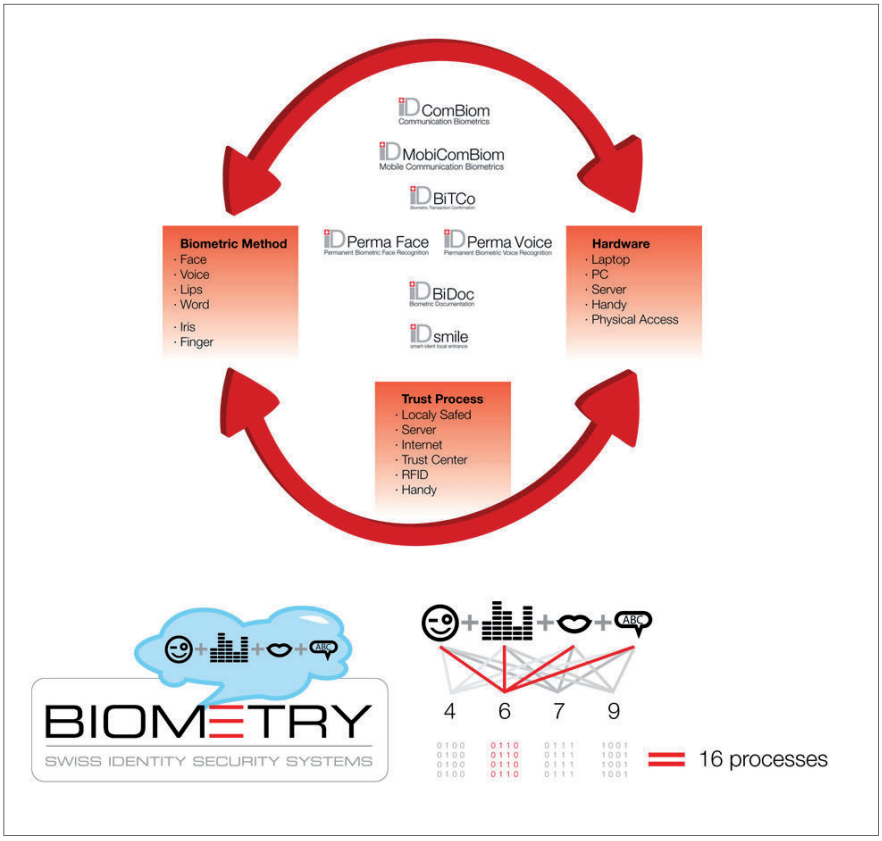


Bild 3: Kombination von unterschiedlichen Methoden, Hardware und Prozessen.

haben, kann er die permanente Authentifizierung einstellen. Das bedeutet, dass im Hintergrund automatisch das Gesicht in regelmäßigen Abständen geprüft wird. Wird der Benutzer nicht erkannt, etwa weil er sich vom Bildschirm abgewendet oder den Platz verlassen hat, schließt das Programm alle geschützten Anwendungen. Kehrt dieser zurück, erkennt ihn das Programm automatisch und alle Anwendungen sind eine Sekunde später wieder sichtbar. Die Sicherheit der Daten ist damit jederzeit gewährleistet und das lästige Computer herunterfahren oder das Schließen aller gesicherten Anwendungen entfällt. Die Software läuft auf jedem Windows-Rechner. Der Benutzer braucht lediglich noch eine Webcam und ein Mikrofon. In den meisten Computer und Laptops ist das heutzutage bereits standardmäßig integriert. Eine 30-Tage-Testversion ist unter www.biometry.com downloadbar.

Die Installation dauert maximal fünf Minuten. Der Anwender muss dann nur noch alle passwortgeschützten Dateien und Anwendungen mit BIOMETRYsso verknüpfen und die Software einlernen. Dafür muss er einfach einige Male in die Kamera schauen und die angegebenen Zahlen nachsprechen. Die aus diesen Daten generierten Templates speichert das Programm im Hintergrund und überprüft die Daten bei jeder Neuanmeldung. Daher ist es von Vorteil auch einige Templates bei schwierigen Lichtverhältnissen oder in lauter Umgebung aufzunehmen. Was tun, wenn die biometrische Authentisierung doch einmal fehlschlägt? Dann hat der Benutzer die Möglichkeit mittels PUK (personal unblocking key) an seine Anwendungen zu gelangen. So mancher Anwender wird diese Prozedur schon von seinem Mobiltelefon her kennen, wenn er dreimal hintereinander die falsche PIN eingegeben hat.

Q & A-Session zum Thema von it security

Je nach biometrischem Verfahren, wird bestimmte Hardware wie eine Webcam für die Erfassung des Gesichtes, ein Mikrofon zur Tonaufnahme, die Tastatur, Druckpads für die Unterschriftenerkennung oder Fingerabdrucksensoren benötigt.

? Warum gibt es so viele biometrische Verfahren und warum setzt jeder Hersteller setzt auf ein anderes?

Der Biometrie-Markt ist aktuell ein so genannter Emerging Market. Das heißt, derzeit befinden sich viele Technologien und Lösungen noch im frühen Stadium der Entwicklung. Es ist daher wichtig, im Vorfeld genau zu prüfen, welche Lösung am Besten in das Sicherheitskonzept des Unternehmens passt. Der Einsatz von biometrischen Systemen im Unternehmen sollte immer eine Ergänzung und kein Ersatz für die üblichen Sicherheitsmethoden sein.

? Ziel sollte es also sein, das Sicherheitslevel zu steigern?

Generell gilt, dass multimodale biometrische Verfahren vorteilhafter sind, denn sie vereinigen die Vorzüge von allen verwendeten Prozessen. Ein Beispiel ist der biometrische Pass, bei dem das biometrische Gesicht, der biometrische Fingerabdruck und in Zukunft auch die biometrische Iriserkennung verwendet werden.
Noch sicherer ist es, wenn die Verfahren simultan abgefragt werden, wie bei einer Video- und Tonaufnahme. Hier ist die Verfahrenskette sehr komplex und daher extrem schwer zu täuschen. Kommt noch ein OTP (one time Passwort) oder Random Challenge Response hinzu, so ist der Datenzugang absolut gesichert. Eine zusätzliche Sicherheit bieten auch Lösungen, die während des Arbeitsprozesses beständig prüfen, ob auch wirklich noch die authorisierte Person am Rechner arbeitet.

? Die Bedienerfreundlichkeit ist nach Ihrer Meinung nach das entscheidende Element?

Umfragen haben ergeben, dass in den Unternehmen die Sicherheit oftmals dem Komfort-Bedürfnis untergeordnet wird. Hier punkten Softwarelösungen, die schnell installiert und eingelernt sind. Und via Single-Sign-On muss der Anwender sich nur einmal anmelden, um auf alle seine geschützten Daten zuzugreifen. Ist die Lösung dann noch intuitiv bedienbar und arbeitet mit vertrauter Hardware wie etwa einer Webcam und einem Mikrofon, steigert das die Mitarbeiterakzeptanz noch einmal deutlich.

? Welche Vorteile bietet die biometrische Authentifikation?

Die biometrische Identifikation erlaubt eine Authentifikation von Personen aufgrund ihrer persönlichen und individuellen Körpermerkmale. Gerade im Zeitalter der modernen Datenkommunikation und des Online-Bankings wird es immer wichtiger, zu wissen, mit wem man es zu tun hat. Jeder, der in den Besitz eines Passwortes oder einer PIN gerät, kann im Namen des Betroffenen handeln und so unberechtigten Zugang erhalten. Dies kann durch den Einsatz von biometrische Identifikationssystemen verhindert werden.

Das Grundprinzip der biometrischen Authentifizierung ist bei allen Lösungen gleich: Zuerst erfolgt die Personalisierung bzw. Registrierung des Nutzers. Als zweites erfasst das System die biometrisch relevanten Eigenschaften der Person. Im Anschluss werden die damit erstellten Datensätze (Templates) mit den zuvor abgespeicherten Daten verglichen. Stimmen diese überein, erhält die Person Zugriff. Eine noch höhere Sicherheit bieten Lösungen, die auch während die Person am Computer arbeitet, bestimmte biometrische Merkmale im Hintergrund regelmäßig verifizieren. Dadurch wird vermieden, dass bei Abwesenheit des Users jemand anderes Dateneinsicht erhält.

? In welche Kategorien kann man biometrische Authentisierungsverfahren einteilen?

Die unterschiedlichen Authentisierungsverfahren werden in mehrere Kategorien eingeteilt:

- Was ich weiß: Hier handelt es sich um Authentisierungsverfahren, bei denen beispielsweise eine PIN (Personal Identification Number) oder Passwörter abgefragt werden. Diese Methode ist sehr leicht fälschbar.
- Was ich habe: Hier wird ein Schlüssel, eine Smartcard oder ein Token verwendet. Bei Verlust oder Diebstahl hat dann aber auch jeder Fremde Zugriff auf die unternehmensinternen Daten.
- Wer ich bin: Unter diesen Bereich fallen biometrische Authentisierungsverfahren: ID-Free HaM (Idendity – Free hands and memory) sowie
- Multi-Level-Verfahren: Mehrere Authentisierungsprozesse werden miteinander kombiniert, beispielsweise Smartcard plus biometrische Gesichtsverifikation.

? Wo liegen die Sicherheitsproblemen eines Authentifizierungssystems?

Die Schwierigkeit besteht darin, dass Authentifizierungssystem so auszulegen, dass die Fehlerrate niedrig und das Sicherheitslevel hoch ist. Zudem sollte sichergestellt sein, dass das System jedes Mal wieder die biometrischen Merkmale der zu authorisierenden Person mit den im System vorhandenen Vorlagen (den sogenannten Referenz-Templates)

überprüft. In der biometrischen Fachsprache werden drei Begriffe unterschieden:

1. FRR (False Reject Ratio): Das Authentifizierungssystem ist so eingestellt, dass die bei der Registrierung erstellte biometrische Datei mit dem Referenz-Template zu 100 Prozent übereinstimmen muss. Damit ist zwar die höchstmögliche Sicherheit gewährleistet; in der Praxis kommt es hier aber zu erheblichen Schwierigkeiten. Hier kann es leicht passieren, dass der Person der Zugang verweigert wird und sie die Authentifizierung mehrmals wiederholen muss, denn biometrische Merkmale verändern sich durch Zeit- und Umwelteinflüsse leicht.

2. FAR (False Acceptance Ratio): Wird der Schwellenwert sehr niedrig eingestellt, erfolgt die Registrierung oft problemfrei. Allerdings nimmt damit auch das Sicherheitslevel ab und es kann vorkommen, dass auch Personen mit vergleichbaren biometrischen Merkmalen Zugriff erhalten.

3. EER (Equal Error Rate): Das ist der Punkt, an dem sich FAR und FRR treffen, wenn sie in Form einer Kurve (Infinitesimalrechnung) gegenübergestellt werden. Je näher dieser Punkt bei Null ist, umso besser ist das biometrische Authentisierungsverfahren.
Generell gilt, dass multimodale biometrische Authentisierungsverfahren vorteilhafter sind, denn sie vereinigen die Vorzüge von allen verwendeten Prozessen. Noch sicherer ist es, wenn die Verfahren simultan abgefragt werden, wie bei einer Video- und Tonaufnahme. Hier ist die Verfahrenskette sehr komplex und daher extrem schwer zu täuschen. Kommt noch, wie eben bereits erwähnt, ein OTP (One Time Passwort), oder Random Challenge Response hinzu, so ist der Datenzugang absolut gesichert.

? Welche biometrischen Merkmale weisen die höchste zeitliche Konstanz auf?

Die Iriserkennung ist am konstantesten. Hier treten die geringsten Veränderungen zwischen dem Zeitpunkt des Einlernens (Enrolment) und den später erfolgenden Registrierungsphasen auf. Bei anderen Verfahren, wie etwa der Gesichtsverifikation, ist es oftmals sinnvoll, das System nach einer Weile wieder auf das leicht veränderte Gesicht – etwa wenn die Person anfängt eine Brille zu tragen oder die Frisur deutlich verändert wurde - einzulernen. Das ist meist schnell erledigt und dauert in der Regel nur ein paar Minuten.

? Welche Organisationen kümmern sich um die Standardisierung biometrischer Systeme? Welche biometrischen Standards gibt es derzeit?

Die ISO (International Standard Organisation) mit der Bestimmung 9303. Im Verbund mit den biometrischen Pässen die ICAO (International Civil Aviation Organisation) mit der Richtlinie 19 794-5 für das Gesicht und 19 794-6 für den Finger.

Was ist der Unterschied zwischen Identifikation und Verifikation? Welche Vorteile hat die Verifikation im Gegensatz zur Identifikation?

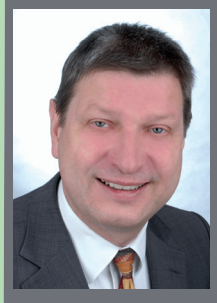
Ziel der biometrischen Erkennung ist stets, die Identität einer Person zu ermitteln (Identifikation) oder eine behauptete Identität zu bestätigen oder zu widerlegen (Verifikation). Identifikation bedeutet 1:n, das heißt ein biometrischen Template wird mit vielen unterschiedlichen gespeicherten Templates verglichen, um die Identität der Person festzustellen.

Verifikation bedeutet 1:1, das heißt ein biometrisches Template wird mit genau einem gespeicherten Template verglichen, um die „behauptete Identität“ zu bestätigen. Diese Methode ist wesentlich schneller und sicherer, es muss allerdings klar hinterlegt sein, wer verifiziert werden soll.

? Wie ist ihr Ausblick in Sachen Biometrie?

Es wird weiter in Richtung Biometrie gehen, gerade auch in der Unternehmens-IT. Vor allem multimodale simultane Biometrie ermöglicht eine Absicherung des PCs, die weit über die üblichen Methoden mittels Smartcard oder Fingerprint hinausreicht. Anstatt der leicht zu knackenden Passwörtern, werden biometrische Single-Sign-On-Lösungen interessant, die bedeutend sicherer und einfach bedienbar sind. Den Zugang zum Computer sowie zu passwortgeschützten Anwendungen erhält dann nur noch die authorisierte Person, deren biometrische Daten wie etwa das Gesicht, die Stimme und das Wort mit den hinterlegten Template-Daten übereinstimmen. Eine noch höhere Sicherheit bieten Lösungen, die auch während die Person am Computer arbeitet, diesen Prüfvorgang im Hintergrund regelmäßig wiederholen. Dabei werden sich zukünftig vor allem biometrische Sicherheitslösungen durchsetzen, die kostengünstig installierbar sind und eine einfache Handhabung bei gleichzeitig höchstem Sicherheitslevel bieten.

Die Fragen stellte: Ulrich Parthier, Publisher, it security



Die Antworten gab: Werner Blessing, CEO der Biometry.com AG