ComConsult Research

Der Netzwerk Insider

Januar 2007

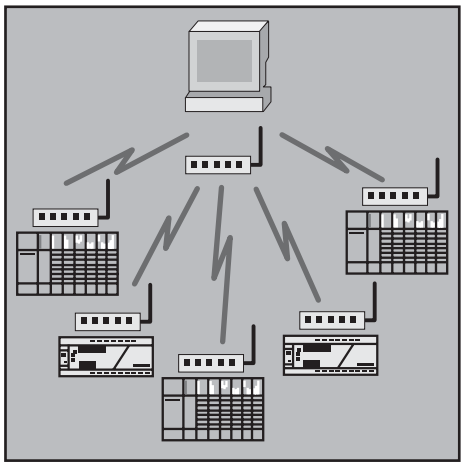
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

SCADA und IT-Security: Informations-Sicherheit in Automatisierungs- und Prozesskontrollsystemen

von Dipl.-Phys. Stephan Beirer

Die moderne IT-Technologie hat in den letzten Jahren auch ihren Weg in die klassische Automatisierungs- und Prozessleittechnik gefunden. Damit kommen die bekannten Hardware- und Software-Komponenten mit all ihren Tücken und Sicherheitsproblemen nun auch in sehr sensiblen Produktionsumgebungen und kritischen Infrastrukturen (KRITIS) zum Einsatz. Darüber hinaus wird auch die Vernetzung von einstmals weitgehend isoliert betriebenen Systemen mit anderen IT-Bereichen immer weiter voran getrieben. Diese unaufhaltsame Entwicklung verlangt dringend nach erweiterten Sicherheitskonzepten, um solch wichtige Ressourcen gegen die neu auftretenden Bedrohungen angemessen abzusichern.



Bei der Steuerung und Überwachung von komplexen industriellen Fertigungsprozessen spielt die elektronische Automatisierungs- und Messtechnik eine wichtige Rolle. Gleiches gilt für die Kontroll- und Leittechnik von räumlich verteilten Systemen wie zum Beispiel Gas- und Ölpipelines, Kommunikations- und Stromnetzen oder Verkehrstelematik-Systemen. Die in diesen Bereichen verwendeten Technologien werden meist unter den Oberbegriffen DCS (Distributed Control Systems) und SCADA (Supervisory Control and Data Acquisition) zusammengefasst.

weiter auf Seite 22

Zweitthema

RAS via VPN - Leitfaden anhand eines Projektbeispiels

von Dipl.-Inform. Andres Meder

Die Nutzung Virtueller Privater Netze (Virtual Private Networks, VPN) hat sich in der jüngeren Vergangenheit insbesondere im Bereich des Remote Zugriffs mobiler oder auch stationärer Anwender (Stichwort: Telearbeit) auf zentrale Ressourcen als mehr oder weniger Standard-Lösungsansatz etabliert.

Wer als Hersteller von Netzwerktechnik - sei es auf dem Infrastruktur- oder auch auf dem Sicherheitssektor - etwas auf sich hält, bietet entsprechende Lösungen mit teilweise üppigem Funktionsumfang an. Gerade dieses umfangreiche Angebot stellt den Netzwerkverantwortlichen, der mit dem Aufbau einer geeigneten Lösung für die jeweiligen Rahmenbedingungen betraut ist, jedoch vor mitunter nicht einfach zu treffende Entscheidungen. Schlagworte sind hier unter anderem: IPSec oder SSL, Security Token oder Smart Cards, transparenter Netzzugriff: ja oder nein, …

weiter auf Seite 9

Top Veranstaltung

ComConsult IT-Sicherheits-Forum 2007

auf Seite 6

Zum Geleit

Asterisk: OpenSource-Telefonie wirklich reif für die Nutzung in Unternehmen?

auf Seite 2

Report des Monats

VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

auf Seite 20

Zum Geleit

Asterisk: OpenSource-Telefonie wirklich reif für die Nutzung in Unternehmen?

Irgenwie war der Wurm drin in unserem technischen Übergang ins neue Jahr. Erst fällt unser Mail-Proxy aus, eigentlich nicht tragisch, da der Telekom-Server für 4 Tage speichert, dann kommt der Telekom-Server nicht damit zurecht, dass unser Backup-MTA nicht verfügbar ist, obwohl unser Primär-MTA einwandfrei arbeitet. Also keine Mails vom 24. bis zum 27.12. Das Problem gerade gelöst, verabschiedet sich die Festplatte unserer TK-Anlage. Eigentlich auch kein Problem, wir haben eine identische Backup-Anlage. Natürlich lässt sich der Lizenz-Key nicht auf die Backup-Anlage übertragen, die Nortel Hotline ist auch nicht gerade hilfreich, aber wer will ihr das zwischen Weihnachten und Neujahr verdenken. Also, wir brauchen schnellstmöglich eine neue TK-Lösung. Da die Ablösung der Nortel-Anlage sowieso für 2007 geplant war, die Hardware bröckelte schon, theoretisch kein Problem.

Aber:

- wie kauft man zwischen Weihnachten und Neujahr eine TK-Anlage, die dann auch sofort zu installieren ist?
- und vor allem welche kauft man? Die Grundsatzentscheidung ist klar und steht seit Wochen fest: die Signalisierung muss auf SIP basieren. Cisco Call Manager Express kommt für uns aufgrund unseres Anforderungsprofils nicht in Frage, nur der Call Manager selber wäre eine Alternative. Aber ein Einstieg vor Version 6 ist sinnlos, wegen SIP. Siemens HiPath 8000 ist ein wenig groß für uns (insbesondere in Kombination mit ACD etc), ähnlich wie bei Cisco würden wir auch hier erst mit Version 3 einsteigen. Nortel wird für uns dann spannend, wenn die Integration mit dem Microsoft OCS erfolgt ist, also erst 2008. Uns so könnte die Liste beliebig weiter gehen
- also schnelle Entscheidung: wir brauchen eine Übergangslösung, die aber alle unsere bestehenden Anforderungen erfüllen soll
- und: wir haben Freitag, den 29.12., die Lösung soll noch vor Silvester laufen. Unmöglich? In der Tat, der Versuch, auf einen Nortel BCM 50 umzusteigen, scheitert an der Nichterreichbarkeit. Und so geht es weiter. Aber siehe da: einer ist erreichbar und er ist auch bereit, am Samstag, den 30.12. zu installieren!!! Und zwar ein Vertreter der Anlage, für die es angeblich keinen geregelten Support gibt

Und so sind wir nun mitten drin in unserem Asterisk-Experiment. Und stellen erst einmal fest:

- hervorragender Service, der Lieferant kommt mit vorinstalliertem IBM-Server, den er noch in der Nacht aufgesetzt hat, inklusive der Konfiguration des S2M-Interfaces
- der Lieferant bietet einen Wartungsvertrag mit hoher Verfügbarkeitszusage
- Grundfunktionalität in wenigen Stunden am laufen inklusive Unified Messaging mit Speicherung von Voice-Mail und Fax auf unserem Exchange-Server

Und nun kommt das erstaunliche: wir sind ursprünglich von einer reinen Übergangslösung ausgegangen, da wir irgendwie intuitiv der Meinung waren, dass Asterisk unsere technischen Anforderungen nicht erfüllt (und die sind trotz der geringen Größe der Installation erheblich). Aber im Moment sieht es so aus, dass dies eine falsche Annahme war. Asterisk hat tatsächlich einen sehr großen Funktionsumfang (wenn ihn denn auch nur jemand im Detail kennen würde, tatsächlich sind viele Funktionen so in den Parameter-Dateien vergraben, dass eine Kenntnis aller Funktionen schwierig ist).
Und so haben wir unsere Entscheidung getroffen: wir werden die Asterisk-Installation weiter betreiben und daraus einen öffentlichen Modellversuch machen (ob das eine Dauerlösung ist, ist noch unklar, vermutlich werden wir im Laufe des Jahres auf eines der Standard-Produkte wechseln, insbesondere wegen der notwendigen Knowhow-Pflege). Den Asterisk-Praxis-Test werden wir mit einem Test der heute Verfügbaren SIP-Funktionalität inkl. der Telefone verbinden. Dies wird unter anderem in unser SIP-Seminar einfließen (nächster Termin im Februar, wird sicher spannend), exklusiv werden wir auf dem Netzwerk-Redesign-Forum insbesondere über den Aspekt von SIP in Netzwerken berichten.

Wir sind noch mitten in den Detail-Konfigurationen, aber schon jetzt kann man folgende Aussagen treffen:

Positives

P1: Asterisk hat einen erheblichen Leistungsumfang

P2: Die Basis-Installation ist einfach und schnell

P3: Die Lösung ist in Verbindung mit dem darunter liegenden Linux sehr flexibel gestaltbar

P4: die auf dem Markt angebotenen Service-Pakete sind ok

P5: Asterisk beinhaltet eine ganze Reihe von wichtigen Voice-Anwendungen wie Queuing, ACD, IVR und UM (die Handhabung eingehender Sprach- und Fax-Nachrichten und deren Weiterleitung an unseren Exchange-Server war überraschend trivial. Asterisk ist für jeden, der eine einfache UM-Lösung sucht, eine echte Option, auch als Ergänzung einer anderen TK-Lösung)

Nachteile

N1: die Asterisk Standard-Konfiguration in den Parameter-Dateien kann nur einem Linux-Freak gefallen. Hier ist eine GUI-Oberfläche zumindest für Standard-Konfigurationen unverzichtbar

N2: es fehlt ein brauchbares Handbuch (es gibt diverse im Internet, aber wir haben bisher nichts wirklich für uns

brauchbares gefunden). Viele Informationen stehen nur als Kommentar in den Parameter-Dateien, eigentlich eine Zumutung

N3: was ist überhaupt Asterisk? Ist Asterisk wirklich OpenSource? Die Urversion kommt von Digium, d.h. eigentlich gibt es drei Versionen, die Digium anbietet. Eine normale OpenSource-Version, Asterisk Enterprise und AsteriskNow als Integration mit einer Linux-Distribution. Auf der OpenSource-Version basieren nun weitere Versionen, zum Beispiel die Trixbox und OpenBPX. OpenPBX zum Beispiel brüstet sich damit, dass sie Digium-spezifische Treiber wieder entfernt haben (was soll das ?????). Auf OpenPBX basieren nun weitere Versionen, die zum Beispiel die Parameter-Dateien neu sortieren, viele Linux-Distributionen haben eine integrierte Asterisk-Version, so auch unsere Debian-Distribution (aber welche denn nun?). Weiterhin unterstützt Asterisk nicht nur SIP sondern arbeitet eigentlich von Hause aus mit einer Digium-spezifischen Signalisierung, OpenSource muss also nicht immer auch OpenProtocol oder Open-Standard bedeuten

N4: Asterisk hat keine Standard-Architektur, die skaliert und mit den Lösungen der traditionellen Anbieter vergleichbar wäre. Das beginnt schon bei der Frage nach Backup und Ausfallsicherheit. Natürlich kann man hier weitgehende Lösungen schaffen, aber diese basieren dann auf Linux-Funktionalität und sind individuelle Lösungen und keine Standard-Lösungen

N5: Asterisk ist im Lowend-Bereich nicht wirklich preiswert. Integriert man die Kosten für Hardware und Konfiguration, ist man im Endeffekt auf den Kosten eines Nortel BCM oder einer Innovaphone. Hintergrund ist hier der Preisverfall im TK-Markt auf der einen und der hohe Asterisk-Konfigurationsaufwand für anspruchsvollere Funktionen auf der anderen Seite

Fragezeichen

Unter Fragezeichen sprechen wir Funktionen an, deren Bewertung uns im Moment unklar ist, diese sind:

F1: Asterisk ist eine Entwicklungsplattform für Sprach-, Präsenz- und Multimedia-Anwendungen. Auf der einen Seite ist es damit sehr mächtig, auf der anderen komplex

F2: viele traditionelle Sprach-Produkte sind auch nicht gerade selbsterklärend in der Konfiguration, und das ist eigentlich eine Untertreibung. Vielleicht sind Anforderungen an Sprach- und Multimedia-Kommunikation einfach komplex und es gibt keine wirklich einfache Lösung?

F3: die Kombination aus Linux und Asterisk beinhaltet viel Potenzial. So werden viele Linux-Freunde das fehlende GUI nicht wirklich als Nachteil empfinden sondern eher die Möglichkeit der Gestaltung eigener und individueller GUI´s hervorheben, ohne Frage ist das in der gegebenen Umgebung einfach und schnell möglich

F4: Asterisk folgt dem Weg, den Apache, MySQL und ähnliche Anwendungen erfolgreich beschritten haben. Wenn die Pflege einer Apache-Konfiguration so marktübergreifend in so hoher Zahl möglich ist, sollte das eigentlich auch für Asterisk möglich sein. Mit Linux und den genannten Applikationen ist eine Knowhow-Basis entstanden, die in den meisten Unternehmen sowieso vorausgesetzt werden muss. Zumindest die Umgebungskomplexität relativiert sich damit

Für uns hat die Sache im Moment Modellcharakter. Zudem wollen wir auch wirklich praxisnah im Tagesbetrieb sehen, wo SIP heute steht.

Was kommt als nächstes:

- wir analysieren verfügbare GUI´s für Asterisk, die sowohl Basiskonfigurations-Aufgaben abdecken als auch weitergehende Funktionen wie Übersicht über eingeloggte Agenten
- wir testen SIP-Telefone. Es ist klar, dass die TK-Leistungsmerkmale, die Asterisk bietet, nur verfügbar sind, wenn auch die eingesetzten Telefone diese Leistungsmerkmale unterstützen. Hier werden Telefone mit programmierbaren Leistungsmerkmalen auf Dauer unverzichtbar werden, dies ist der Weg, den Cisco erfolgreich mit seinen Telefonen vorgezeichnet hat. Mit der Programmierbarkeit der Leistungsmerkmale wird eine erhebliche und nicht zu unterschätzende Investitionssicherung erreicht
- wir machen den Vergleich: sind auf dem Markt frei kaufbaren SIP-Telefone wirklich eine Konkurrenz für die SIP-Telefone der traditionellen Anbieter, hier speziell Cisco, Nortel und Siemens? Immerhin geht es auch um Sprachqualität und individuelle Konfiguration von Leistungsmerkmalen. Wir arbeiten erst einmal mit dem Snom 360, haben aber die angesprochenen Hersteller um Testgeräte gebeten, um einen Testvergleich durchführen zu können. Hinzu werden noch die neuen Telefone von Polycom kommen, wir hoffen, dass wir eins der neuen 650er bekommen können. Aber schon in der Erwähnung des 650 wird klar, dass Anlagen-ungebundene SIP-Telefone nicht unbedingt preiswert sein müssen (es gibt keinen mir bekannten offiziellen Preis des 650 für Europa, aber ich vermute, er wird ähnlich wie das 601 im Listenpreis zwischen 400 und 500 Euro liegen)

Kann Asterisk einen Call-Manager oder eine HiPath 8000 ersetzen? Trotz der Entscheidung der Universität Huston, Asterisk für 6000 Teilnehmer einzusetzen, sind wir der Ansicht, dass es für große Kunden noch nicht geeignet ist. Hinzu kommen die skalierbare Anlagenarchitektur, die weitergehenden Leistungsmerkmale, die vielen verfügbaren Zusatz-Applikationen dieser Anlagen. Aber wir werden sehen. Auf jeden Fall kann Asterisk aber auch für diese Produkte ggf. eine interessante Ergänzung sein. Es gibt große Projekte, in denen durch die Ergänzung durch Asterisk speziell für Voice-Mail und Fax erhebliche Geldsummen eingespart werden konnten.

Bisher verläuft der Test überraschend positiv. Wir streben auf der anderen Seite für 2007 auch einen Test der HiPath 8000 an. Ich bin überzeugt davon, dass sich an diesem Produkt das Schicksal von Siemens-Com entscheiden wird. Hinzu kommt, dass Siemens Marktführer in Deutschland ist, das Zukunftsprodukt des Marktführers hat naturgemäß einen sehr hohen Stellenwert für den deutschen Markt. Betrachtet man die technische Entwicklung der letzten 2 Jahre, so ist hier auch eine deutliche Weiterentwicklung zu sehen.

Sie sehen, das neue Jahr hat turbulent begonnen. Wir hoffen, dass wir Ihnen in den nächsten Wochen wichtige Informationen für Ihre Projekte und Entscheidungen liefern können. Versäumen Sie unter diesem Blickwinkel nicht, sich rechtzeitig einen Platz auf dem Netzwerk-Redesign Forum 2007 zu sichern. Schon jetzt zeichnen sich angeregte und wichtige Diskussionen für diese Veranstaltung ab. Wir werden exklusiv über den Stand unserer Testarbeiten berichten und auch die betroffenen Hersteller in die Diskussion auf der Veranstaltung einbinden.

In diesem Sinne
auf ein spannendes Jahr 2007

Ihr Dr. Jürgen Suppan

TOP-Veranstaltung zum Megathema 2007

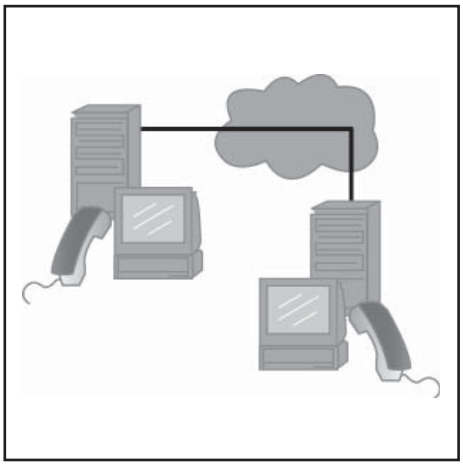
Top Thema: SIP - Basis-Technologie der IP-Telefonie

Wenige Standards in der Geschichte der TK, der Netzwerke und der IT werden unsere Branche so verändern wie das Session Initiation Protocol SIP. Der Wechsel von Cisco und Siemens zu SIP mit dem CallManager 6 und der HiPath 8000 unterstreichen das genauso wie der Einstieg von Microsoft zusammen mit Nortel in diesen Markt.

Die Konsequenzen eines offenen Standards sind erheblich, auch wenn die Produkte von den traditionellen TK-Anbietern kommen:

- Ein zunehmendes Angebot offener Sprach- und Multimedia-Applikationen für ACD, IVR, UM und weitere Spezialanwendungen
- Freie Wahl von Endgeräten (abhängig von gewünschten Funktionsmerkmalen)
- Freie Wahl von Gateways
- Es entstehen standardisierte Entwicklungs-Umgebungen für Sonderlösungen: Cisco zeigt mit IPICS und der Integration von Funk, Sensoren, Sprache, Meldetechnik welchen gigantischen Umfang solche Lösungen haben können

In der näheren Analyse zeigen sich für nahezu alle Unternehmen die enormen Vorteile einer offenen Sprach- und Multimedia-Welt. Ein typisches Beispiel dafür ist Asterisk, der als offene Lösung nicht nur SIP-Telefonie implementiert sondern einen umfassenden Baukasten für ACD, Queuing, Voice-Mail und Unified Messaging sowie für individuelle Entwicklungen bietet. Allein in der Ergänzung traditioneller TK-Lösungen durch Asterisk liegt ein hohes Potenzial an Funktionalität zu so geringen Kosten, dass alleine dieser Aspekt fast einer Revolution gleichkommt.



SIP ist ohne Frage eines der, wenn nicht das Megathema des Jahres 2007. Nach wie vor wird dabei insbesondere der Leistungsumfang von SIP weit unterschätzt. Auch so verbreitete Implementierungen wie Asterisk oder SER werden in ihrer Nutzbarkeit häufig falsch eingeschätzt.

Hier setzt unser hochaktuelles Seminar zum Thema SIP an. Es erläutert die Hintergründe von SIP und es zeigt auf, wie weit diese Lösungen gehen können. Wir zeigen an Beispielen typische Implementierungen. Und wir stellen uns der Diskussion über unseren Modellversuch, bei dem wir unsere TK-Lösung durch Asterisk ersetzt haben, für jeden, der unsere Anforderungen kennt, sicher eine Überraschung. Nutzen Sie die einmalige Gelegenheit, sich in diesem Seminar über Theorie und Praxis von SIP informieren zu lassen.

Natürlich erhalten Sie auch Informationen über die Haltung der großen Hersteller zu dem Thema, die wie oben schon erwähnt entweder schon den Weg zu SIP eingeläutet haben oder dies in den nächsten Monaten tun werden.

Ein Top-Seminar zum Megathema des Jahres. Sichern Sie sich rechtzeitig einen Platz.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

SIP - Basis-Technologie der IP-Telefonie

☐ Ich buche das Seminar
SIP - Basis-Technologie der IP-Telefonie
05.02. - 07.02.07 in Bonn
zum Preis von € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____07

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Aktueller Kongress

Netzwerk-Redesign Forum 2007

Die ComConsult Akademie veranstaltet vom 23. - 26.04.2007 ihren Kongress „Netzwerk-Redesign Forum 2007“ in Königswinter.

Auch in diesem Jahr greift das Netzwerk-Redesign-Forum die aktuellsten Trends der Netzwerk-, TK- und vernetzten IT-Welt auf, analysiert neue Technologien und gibt wichtige Empfehlungen für den Betrieb und die Planung von Netzwerken.

Eine Auswahl der Themen:

1) Netzwerke 2007/2008: Trendanalyse
Dr. Suppan stellt die aktuelle Markt- und Technologie-Analyse von ComConsult-Research vor

- Mehr Bandbreite im WAN und die Folgen
- Konsumerverhalten beeinflusst Unternehmenstechnik
- Parallele kontra hierarchische Systemarchitekturen im Netzwerk
- Neue Webtechnologien und ihr Einfluss
- Sprach- und Multimedia-Kommunikation im Netzwerk
- Wo stehen wichtige Hersteller, welchen Weg gehen sie
- TK-Markt vor der Entscheidung: nicht alle werden überleben

2) Netzwerk-Design 2007

Frau Borowka stellt die aktuellesten und neuesten Trends des Netzwerk-Design vor. Im Schwerpunkt Echtzeitdienste und ihr zunehmender Einfluss auf das Design und den Betrieb, Monitoring von QoS-Betriebssituationen

3) TCP/IP unter Druck

Das Research-Team der ComConsult Beratung und Planung analysiert unter der Leitung von Oliver Flüs die aktuellsten und gravierendsten Änderungen im Betrieb von TCP/IP: Verdopplung bis Verdreifachung des Adressbedarfs, Auswirkung von SIP-Trunks zu Providern auf die Adressgestaltung, Probleme mit privaten Adressräumen, IPv6 ante Portas – was ist wann zu tun, Herausforderung und Sanierungsbedarf: Standort-übergreifendes Management von DNS und DHCP

4) Netzwerk-Trennung mit Tücken

Dr. Moayeri präsentiert die neuesten Untersuchungs-Ergebnisse zum Thema Netzwerk-Trennung, angefangen von der Trennung von Daten und Sprache bis hin

zur Vermeidung von Desastern: VLAN-Konzepte und ihre Tücken: wohin mit Softphones/ Sprachapplikationen auf dem PC/ Datenapplikationen auf dem Telefon, warum einfache VLAN-Layer3-Integrationen unzureichend sind

5) Netzwerk-Sicherheit

Dr. Hoff analysiert Vor- und Nachteile verschiedener Sicherheits-Ansätze. Warum weder reine Netzwerk- noch reine Desktop-Konzepte tragfähig sind. Wo die Grenzen und Probleme von IEEE 802.1X liegen. Herr Nispel geht auf die NAC-Ansätze der verschiedenen Hersteller ein und bewertet Vor- und Nachteile.

6) WAN im Wandel

Dr. Moayeri präsentiert aktuelle Ergebnisse zum Thema Weiterentwicklung und Anpassung von WAN-Netzwerken, beginnend bei der Optimierung bestehender Strukturen und endend mit Trends in der Planung und Ausschreibung.

7) Auswahl neuer Switch-Systeme

Herr Kell analysiert die Kriterien zur Auswahl neuer Switchsysteme, speziell für den Workgroupbereich. Zunehmender Bandbreitenbedarf, mehr Ausfallsicherheit, Handhabung von PoE: wie sieht der Weg zum besten Switch aus.

8) Verkabelung 2007

Verkabelungslösungen unterliegen permanenten Verbesserungen, Produkte und Messtechnik befinden sich in der Evolution. Wie sehen aktuelle Lösungen mit Kabeln/Steckern/Frequenzen aus, welche Messtechnik ist notwendig. Lassen sie sich auf den neuesten Stand von Kabeln bringen.

9) Wireless-LAN vor dem Bruch

Dr. Hoff geht auf die sich immer mehr andeutende Revolution im Wireless LAN-Bereich ein. Mit Apple und D-Link haben in der zweiten Januar-Woche die ersten Massenhersteller echte, ernstzunehmende 801.11n-Implementierungen für Q1/Q2 angekündigt. Beide unterstützen 2,4 und 5 GHz, D-Link mit Dual-Radios und 3 MIMO-Antennen. Die Konsumerwelle rollt an, wie die CES in Las Vegas wieder gezeigt hat. Parallel bringen nahezu alle Hersteller neue Architekturen und Produkte auf den Markt. Wireless Switches werden zum Standard für große Unternehmen. Unsere Top-Analyse zum Wireless-Markt gibt Ihnen die Entscheidungsbasis, die Sie brauchen.

10) MESH-Netzwerke: Wandel der Denkweise

Frau Borowka berichtet über den neuesten Trend mit MESH-Netzwerken. Hin zu selbst konfigurierenden, vermaschten Distributionssystemen hoher Bandbreite und maximaler Verfügbarkeit. Die Vision des automatisch Bandbreiten-angepassten Netzwerks durch Clients als variable Knoten.

11) SIP: der neue Standard für Sprach- und Multimedia-Kommunikation

Der Workshop von Frau Borowka analysiert Vorteile und Defizite von SIP gegenüber traditionellen Sprachlösungen. Die Ergebnisse der neuesten ComConsult-Research-Studie werden exklusiv auf dem Forum vorgestellt.

Weitere Themen sind in der Entwicklung. Auch in diesem Jahr trifft sich die Branche auf diesem herausragendem Forum, das in einer einzigartigen Mischung aus Analysen, Vorträgen, Ausstellung, Workshops und Diskussion ein Muss für jeden Planer und Betreiber ist. Sichern Sie sich rechtzeitig einen Platz in unserer Top-Veranstaltung des Jahres 2007.

Die Moderation übernimmt Dr. Jürgen Suppan. Er gilt als einer der führenden deutschen Berater für Kommunikationstechnik. Unter seiner Leitung wurden diverse Netzwerkprojekte aller Größenordnungen erfolgreich umgesetzt. Seine Seminare zählen durch ihren didaktischen und lebendigen Aufbau und ihre Praxisnähe und Herstellerneutralität zu unseren erfolgreichsten Veranstaltungen.

Security-Kongress des Jahres

IT-Sicherheits-Forum 2007

Die ComConsult Akademie veranstaltet in Zusammarbeit mit der GAI NetConsult unter der fachlichen Leitung von Dipl.-Inform. Detlef Weidenhammer vom 07.05. - 10.05.07 ihren Kongress „IT-Sicherheits-Forum 2007“ in Königswinter.

Das IT-Sicherheits-Forum 2007 hat sich in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen wird mit einführenden Tutorien, technischen Workshops und Fachvorträgen zu aktuellen und zukünftigen Entwicklungen für jeden Interessierten etwas geboten. Dabei wird äußerst hoher Wert auf Praxisnähe gelegt, die Teilnehmer sollen die gewonnenen Erkenntnisse möglichst sofort in der eigenen Umgebung anwenden können. Das Gesamtprogramm umfasst in diesem Jahr:

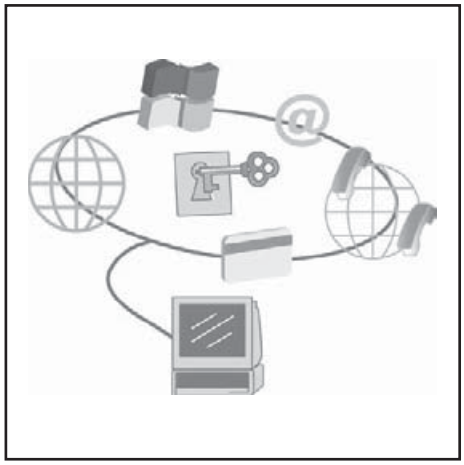
- Aufzeigen der aktuellen Trends bei Bedrohungen und Schutzmaßnahmen
- Vorstellung und Bewertung neuer Sicherheitstechnologien
- Moderierte Workshops mit Produktvergleichen und Live-Demos
- „Best Practice“ Sessions mit Sicherheitsempfehlungen für den Tagesbetrieb
- Tutorien und Seminare für Anfänger und Fortgeschrittene

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren. Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle Fachthemen analysiert und auch Praxisszenarien vorgestellt. Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu aktuellen Sicherheitsthemen vorbehalten. Da diese in Vor- und Nachmittagssitzungen parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Als Themen des IT-Sicherheits-Forums 2007 sind bisher u.a. vorgesehen:

Welche Bedrohungen erwarten uns in 2007?
- Starkes Anwachsen von 0-Day Attacken
- MS-Office erneut im Fokus der Hacker
- Metasploit Framework zur einfachen Exploit-Entwicklung
- Neue Schwachstellen bei drahtlosen Komponenten und Mobiles

Windows Vista unter Sicherheitsaspekten
- Neues: Vom BitLocker bis zum UAC (User Account Control)



- Auswirkungen der neuen Kernel-Protection auf andere Sicherheitsfirmen
- Empfehlungen zur Einsatzplanung im Unternehmensumfeld
- Bewertung der bisher bereits bekannt gewordene Sicherheitslücken

Sicherheit in Automatisierungs- und Prozesskontrollsystemen (SCADA)
- Problembereiche von Produktionsumgebungen und kritischen Infrastrukturen
- Anfälligkeit gegen interne und externe Bedrohungen
- Analyse einiger bekannt gewordener Vorfälle
- Ableitung von Richtlinien für SCADA-Systeme

Erstellung und Betrieb von sicheren Webanwendungen
- Überblick zu Gefahren durch neue Angriffstechniken
- Ergebnisse von Scan- und Penetrationstests
- Sicherheitshinweise für Entwickler von Webanwendungen
- Bewertung des Einsatzes von Application Firewalls

Erhöhte Anfälligkeit der IP-Infrastruktur
- Zunahme von Erpressungen mit DDoS-Attacken
- DNS-Angriffe auf lokale und globale Netzstrukturen
- Manipulation von Routing-Informationen
- Globale Gefahren durch riesige Botnets

Content-Security: Umgang mit gefährlichen Inhalten
- Spyware läuft Viren und Würmern den Rang ab
- Umgehung der Firewallkontrollen mit „durchtunnelnden“ Anwendungen
- Müssen Handyviren stärker beachtet werden?
- Was liefern aktuelle Content-Filter?

Zugangskontrolle zum Unternehmensnetz
- Notwendige Schutzfunktionen am Endpoint
- Anforderungen an das zentrale Management solcher Lösungen
- Endpoint Security Enforcement
- Cisco-NAC vs Microsoft-NAP

Physische Sicherheit in IT-Umgebungen
- Haftungsrisiken für IT-Verantwortliche
- Sicherheit in der Bauausführung und Infrastruktur
- Sichere Ausführung von Energieversorgung, Zugangs- und Brandmeldetechnik
- Technische Sicherheit der IT-Komponenten

Einschätzungen zu Standards im Sicherheitsbereich
- BSI- und / oder Internationale Standards
- Sicherheitsmanagement nach ISO 27001
- Best Practices für Notfallplanung mit ISO 17799 und ITIL
- Welche Kombinationen von Standards haben sich durchgesetzt?

Compliance / Risk Management
- Berücksichtigung staatlicher, industrieller und rechtlicher Vorgaben
- Einschätzung der RM-Ansätze von BSI und ISO
- Risikoindikatoren und Aufbau eines Frühwarnsystems
- Business Continuity als wichtiger Bestandteil des RM

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen und Praxis-Demos hat seinen hohen praktischen Wert für die Teilnehmer bewiesen. Daneben werden auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in die Geschäftsabläufe, da hier noch immer die größten Defizite anzutreffen sind. Damit bietet das IT Sicherheits-Forum für Sicherheitsverantwortliche, aber auch für vorrangig technisch interessierte Teilnehmer eine Fülle wertvoller Informationen.

Anmeldungen Kongresse Frühjahr 2007

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2007

☐ Ich buche den Kongress
Netzwerk-Redesign Forum 2007
vom 23.04. - 26.04.07 in Königswinter
inkl. Intensiv-Training am ersten Tag
zum Preis von € 2.190,- zzgl. MwSt.

☐ vom 24.04. - 26.04.07 in Königswinter
ohne Intensiv-Training am ersten Tag
zum Preis von € 1.790,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult IT-Sicherheits-Forum 2007

☐ Ich buche den Kongress
ComConsult
IT-Sicherheits-Forum 2007
vom 07.05. - 10.05.07 in Königswinter
inkl. Tutorium am ersten Tag
zum Preis von € 1.990,-* zzgl. MwSt.

☐ vom 08.05. - 10.05.07 in Königswinter
ohne Tutorium am ersten Tag
zum Preis von € 1.590,-* zzgl. MwSt.

☐ mit Report „Sicherheit in Enterprise-Netzen durch den Einsatz von 802.1X“
zum Sonderpreis von nur € 338,-

Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____07

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Stellenanzeige

Stellenangebot: Netzwerk- und System-Spezialist

ComConsult-Research/ComConsult Technologie-Information GmbH sucht für ihren Labor- und Vortragsbereich einen

Netzwerk- und System-Spezialisten

Wir erwarten folgende Qualifikation:

- Gute bis sehr gute Kenntnisse in aktuellen Netzwerk-Technologien, insbesondere Ethernet, TCP/IP, Wireless LAN
- Gute Kenntnisse in Konfiguration und Betrieb aktiver Netzwerkkomponenten (Cisco, Enterasys, Extreme)
- Gute bis sehr gute Kenntnisse in Windows- und Linuxbasierten Betriebssystemen
- Gute Kenntnisse in Voice over IP, SIP und Telekommunikation

Die Stelle umfasst folgende Tätigkeiten:

- Unterstützung beim Betrieb der hausinternen Netzwerk- und Systemlandschaft
- Eigenständige Durchführung von Produkttests und Analysen (nächste Themen: Mitwirkung beim SIP/Asterisk und HiPath 8000-Test)
- Vorbereitung und Durchführung von Vorträgen und Seminaren
- Verfassen von Artikeln und Reports zu aktuellen Themen
- Mitarbeit bei der Vermarktung und Positionierung unserer Produkte

Wir unterstützen unsere Kunden bei der Auswahl von Technologien und Produkten im Netzwerk- und Systembereich. Unser Ziel ist es, Neuentwicklungen frühzeitig zu bewerten, auf Risiken und Chancen neuer Techniken rechtzeitig hinzuweisen. Sie sollten daher aufgeschlossen gegenüber neuen Technologien sein und den permanenten Weiterentwicklungen im Markt mit Spannung und Neugierde entgegen sehen. Dementsprechend ist diese Stelle mit permanenter Weiterbildung verbunden. Sie arbeiten eng mit einem Team ausgewiesener Experten, eine ausgeprägte Teamfähigkeit ist daher unverzichtbar. Erfahrungen aus der Praxis sind von Vorteil.

Ihre Bewerbung richten Sie bitte an:

ComConsult Technologie Information GmbH
Laborleiter
Dipl.-Math. Cornelius Höchel-Winter
Pascalstr. 25 - 52076 Aachen

Telefon 02408-955-400
Fax 02408-955-399
choechel@comconsult-research.de
http://www.comconsult-research.de

ComConsult Technologie Information

ComConsult Research

Zweitthema

RAS via VPN - Leitfaden anhand eines Projektbeispiels

Fortsetzung von Seite 1

Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Dieser Artikel versucht, auf Basis aktueller Projekterfahrungen einen Leitfaden für den oben erwähnten Verantwortlichen zu erstellen, mit dessen Hilfe für die allermeisten Szenarien eine sinnvolle Lösung aufgebaut werden kann. Dazu werden diverse grundsätzliche Fragestellungen, die in derartigen Realisierungsprojekten häufig auftauchen, diskutiert und - hoffentlich - hinreichend beantwortet. Den Abschluss bildet ein kurzer Blick auf ein beispielhaftes auf der Basis dieses Leitfadens abgewickeltes Planungsprojekt, das in ähnlicher Ausprägung tatsächlich realisiert worden ist.

Zusätzlich zu den diskutierten Aspekten ist natürlich - auch wenn auf diesen Bereich hier nicht im Detail eingegangen wird - wie bei jedem Konzept zunächst eine Analyse des Status Quo und der Vorstellungen bzw. Wünsche hinsichtlich der zu entwickelnden Lösung voranzustellen. Diese Ist- und Anforderungsanalyse ist wesentlicher Eckpfeiler jedweder Konzeption und Planung und sollte daher keinesfalls als unangenehme „langweilige“ Begleiterscheinung des ansonsten „spannenden“ Projekts angesehen werden. Andernfalls ist die Gefahr groß, dass man mit der neu konzipierten Lösung nicht allzu lange wirklich glücklich wird…

Wie können die Sicherheitsziele erreicht werden?

Für die Konzipierung von Kommunikationslösungen sind regelmäßig folgende Sicherheitsziele zu unterstellen:

- Vertraulichkeit (von übertragenen bzw. gespeicherten Informationen)
- Integrität (von Systemen bzw. übertragenen oder gespeicherten Informationen)
- Verfügbarkeit (von Systemen bzw. nachgefragten Informationen)

Eine zu konzipierende VPN-Lösung trägt diesen Sicherheitszielen sinnvollerweise wie folgt Rechnung:

Sichere VPN-Lösungen basieren auf dem Aufbau von Kommunikationstunneln zwischen den beteiligten Partnern (Einzelplatz-Client bzw. Remote Netz sowie internes Netz des zentralen Standorts) über das Internet. Für diese Tunnel wird ein Mechanismus verwendet, der durch Anwendung hinreichend starker kryptografischer Methoden sowohl die Vertraulichkeit der übertragenen Informationen als auch deren Integrität sicherstellt. Hierfür finden Verschlüsselungsalgorithmen sowie Prüfsummenverfahren Verwendung.

Zur Sicherstellung der Vertraulichkeit und Integrität gespeicherter Informationen und von Systemen (innerhalb des internen Netzes) verwendet eine solche VPN-Lösung üblicherweise Filtertechniken, die Zugriffe auf das interne Netz ohne Verwendung der zugelassenen VPN-Tunnel verhindern. Hierfür werden klassische Paketfilter (z.B. Access Control Lists) eingesetzt, die jegliche Kommunikation verwerfen, die nicht zu bestehenden VPN-Tunneln gehört oder für den Aufbau solcher Tunnel notwendig ist. Zur Prüfung, inwieweit VPN-Tunnel zulässig sind, werden als hinreichend stark eingeschätzte Methoden zur Authentifizierung der jeweiligen Kommunikationspartner eingesetzt - hierunter können durchaus unterschiedene Methoden verstanden werden:

Im Falle von Client-PCs, die einen Tunnel zum internen Netz aufbauen (Client-to-Site-Szenario) kommen hierzu grundsätzlich SmartCards oder Security-Token in Frage - von der Nutzung einfacher „Nutzername / Kennwort“-Kombinationen ist in der Regel abzuraten, da eine sichere Wahl derartiger Passwörter für sämtliche Konten in der Praxis unmöglich zu gewährleisten ist. Die Vorgabe komplexer Regeln zur Generierung solcher Passwörter ist hier eher kontraproduktiv, da die Neigung der Anwender, die Passwörter niederzuschreiben, umso größer ist, je komplexer und damit schwerer im Gedächtnis zu behalten diese sind. Mindestens in Szenarien, in denen davon auszugehen ist, dass auch Zugriffe von beliebigen Client-Systemen aus erfolgen müssen (z.B. aus Internet-Cafés), ist dem Ansatz des Security-Tokens jedoch eindeutig der Vorzug gegenüber der SmartCard zu geben. Bei diesen Token handelt es sich um tragbare Passwortgeneratoren, mit deren Hilfe sich der Besitzer beim Aufbau des VPN-Tunnels durch Eingabe des generierten Einmal-Passwortes - in der Regel in Verbindung mit einer nur ihm bekannten PIN - eindeutig ausweisen kann. Über den Einsatz im Rahmen der VPN-Lösung hinaus lassen sich Security-Token praktisch überall einsetzen, wo eine Kennwort-basierte Benutzerauthentifizierung vorgesehen ist, und bieten somit erweitertes Nutzungspotenzial.

Zusätzlich zur Authentifizierung des jeweiligen Benutzers sollte ggfs. eine hinreichend sichere Identifizierung von Clients auf Basis von Managed PCs (s.u.) möglich sein, dies kann durch eine Systemauthentifizierung beispielsweise auf Basis von Zertifikaten erfolgen.

Wird der Tunnel zum internen Netz nicht vom Client-PC des Anwenders, sondern von einem vorgelagerten System (VPN-Gateway) aufgebaut, kommt der Einsatz von Security-Token aus technischen Gründen i.d.R. nicht in Frage, da diese das Ablesen und Eingeben des Einmal-Passworts durch einen Nutzer erfordern. Hier reicht

jedoch die Verwendung hinreichend langer und komplex aufgebauter statischer Passwörter zur Authentifizierung aus, da die Nachteile statischer Passwörter (zu geringe Länge und Komplexität, absichtliche oder fahrlässige Preisgabe durch den Anwender) nicht zum Tragen kommen. Solche Passwörter sollten „zufällig“ generiert werden; ihre Länge sollte dabei mindestens 12 Zeichen betragen. Eine regelmäßige Änderung in kurzen Intervallen ist normalerweise nicht erforderlich, da etwaige Versuche, das Passwort durch Raten in Erfahrung zu bringen, durch zu lange Zeitdauer und zwangsläufige Entdeckung zum Scheitern verursacht sind.

Die dargestellten Maßnahmen werden sinnvoll ergänzt durch eine Kanalisierung der Zugriffsrechte. Hierzu lässt sich ein zusätzlicher Filter einsetzen, der je nach Identität des Anwenders den Zugriff auf bestimmte interne Ressourcen freigibt oder sperrt (Firewallfunktionalität; s.u.).

Maßnahmen zur Sicherstellung der Verfügbarkeit von Systemen oder Informationen im internen Netz durch die VPN-Lösung müssen sich naturgemäß auf den Kommunikationspfad beschränken; die Systeme und Informationen selbst können hier nicht berücksichtigt werden. Die Verfügbarkeit des VPN-basierten Zugriffs hängt von vielen Faktoren ab; zu den wesentlichen hier zu berücksichtigenden zentralen Faktoren zählen:

- das zentrale VPN-Gateway,
- die Anbindung dieses VPN-Gateways an das interne Netz,
- die Anbindung des VPN-Gateways an das Internet.

Die beiden letzten Faktoren sollen hier nicht weiter betrachtet werden. In den meisten Fällen muss hier bei der Konzipierung einer VPN-Lösung auf die bereits vorhandenen Rahmenbedingungen Rücksicht genommen werden; eine komplette Neuplanung der besagten Schnittstellen kommt eher selten in Betracht.

Je nach den zu berücksichtigenden infrastrukturellen Gegebenheiten kommen für das VPN-Gateway - in Abhängigkeit von der konkreten Lösung - verschiedene Ansätze zur Verfügbarkeitssicherung in Betracht. Zu den gängigsten zählen:

- Einsatz einer Cluster-Lösung
- Einsatz einer Hot-Standby-Lösung
- Einsatz von Load-Balancern
- Einsatz dynamischer Routing-Mechanismen
- Definition alternativer Peers in den jeweiligen Gegenstellen
- Bereithaltung eines identischen Reserve-Systems (Cold Standby)

Je nach konkreten Anforderungen reicht häufig zunächst ein Cold Standby-Ansatz aus. Die konzipierte Lösung sollte jedoch grundsätzlich zumindest die Option auf einen höherwertigen Ansatz bieten; insofern ist bei der Evaluierung von Produkten auf entsprechende Möglichkeiten zu achten.

Wie lassen sich bei Bedarf Hersteller- und Produktneutralität sicherstellen?

Eine strikte Neutralität hinsichtlich der beim Aufbau der Lösung einzusetzenden Produkte bzw. deren Herstellen ist üblicherweise nur im Bereich der Ausschreibung durch öffentliche Auftraggeber zu wahren. Ist ein entsprechender Bedarf - aus welchem Grund auch immer - gegeben, so sollte folgendes beachtet werden:

Alle durch das Konzept an eine konkrete Lösung gestellten Anforderungen sind grundsätzlich produkt- und herstellerneutral zu formulieren. Wird in Einzelfällen dennoch auf bestimmte Hersteller oder deren Lösungen Bezug genommen, so sollte darauf hingewiesen werden, dass dies stets als beispielhafte Nennung einer denkbaren Lösung zu verstehen ist. Im Bereich öffentlicher Ausschreibungen ist diese Vorgehensweise übrigens - spätestens bei Formulierung der Leistungsbeschreibung - als ultima ratio zu verstehen, d.h. dergleichen ist nur dann vergaberechtlich zulässig, wenn auf andere Weise (also durch allgemeine Begriffe) eine hinreichend genaue Beschreibung der gewünschten Leistung nicht möglich erscheint.

Derartige beispielhafte Lösungsansätze können im Übrigen während der Konzipierungsphase gleichzeitig dem Nachweis dienen, dass die jeweils konzipierte abstrakte Lösung auch tatsächlich auf der Basis marktverfügbarer Produkte realisierbar ist.

Wie kann ein sicherer Remote-Zugriff sowohl durch eigene Mitarbeiter als auch durch Fremdfirmen erfolgen?

Ein geeignetes VPN-Konzept, wie es das Ziel dieses Leitfadens ist, sollte den Remote-Zugriff durch unterschiedliche Nutzergruppen unterstützen; hier sind insbesondere eigene Mitarbeiter und Fremdfirmen zu unterscheiden. Dazu bieten sich folgende Mechanismen bzw. Ansätze an:

- Einsatz eines Filtermechanismus zur Steuerung des Zugriffs auf interne Ressourcen (s.o.)
- Ermöglichung unterschiedlicher Zugriffsszenarien je nach Nutzergruppe und Nutzungsverhalten

Ansatz 1: Steuerung des Zugriffs

Der Zugriff auf interne Ressourcen wird üblicherweise mittels Firewalltechnik gesteuert: ein geeignetes Filterelement - typischerweise auf Basis eines Paketfilters - lässt Zugriffe auf interne Systeme über bestimmte Dienste je nach Nutzergruppe zu oder sperrt diese.

Für diese Aufgabe kann prinzipiell eine vorhandene Internet-Firewall verwendet werden; günstiger ist es jedoch zumeist, diese Aufgabe dem zentralen VPN-Gateway zu übertragen. Hierdurch ist u.a. eine bessere benutzerbezogene Steuerung möglich (s.u.). Die Lösung (d.h. das als VPN-Gateway einzusetzende Produkt) sollte daher eine derartige Steuerungsmöglichkeit bieten.

Zu beachten ist, dass sich die Steuerung in Abhängigkeit von der Art des Zugriffs (s.u.) unterschiedlich darstellt:

- Bei Client-to-Site-Zugriffen werden die Zugriffsregeln an den jeweiligen Benutzer (bzw. die jeweilige Benutzergruppe) gebunden - nur einem entsprechend berechtigten und authentifizierten Benutzer wird der Zugriff auf die gewünschten Ressourcen gestattet.

- Bei Site-to-Site-Zugriffen werden die Zugriffsregeln an das jeweilige Remote-Netz gebunden - jedem aus diesem Netz zugreifenden Benutzer wird der Zugriff im Rahmen der für das Remote-Netz geltenden Berechtigungen gestattet. Es sind daher bei Fremdzugriffen entsprechende organisatorische Maßnahmen in Form vertraglicher Regelungen zu ergreifen, um einen Missbrauch der so geschaffenen Netzverbindung hinreichend unwahrscheinlich zu machen. Dies gilt im Übrigen stets bei Site-to-Site-Zugriffen, unabhängig von deren technischer Realisierung; insofern ist diese Problematik auch dann gegeben, wenn etwa für derartige Zugriffe eigenständige Lösungen (z.B. eine Dial-In-Lösung) eingesetzt werden.

  Grundsätzlich ist eine benutzerbezogene Filterung für solche Szenarien zwar denkbar - dazu ist eine Authentifizierung des Anwenders gegenüber dem Filter erforderlich - wird in der Praxis jedoch ohnehin meist „unterlaufen“, indem die notwendigen Identitätsausweise (Security Token) innerhalb von Nutzergruppen weitergegeben werden. Dies ist gerade bei Wartungsfirmen gängige Praxis, da eine feste Bindung einer oder weniger Personen des Service-Teams an den Kunden weder machbar noch in dessen Sinne. Üblicherweise erhielte daher schon aus Gründen der Minimierung von Kosten und Administrationsaufwand die Wartungsfirma ein für jeden Techniker frei zugängliches Gemeinschaftstoken; damit ist aber gegenüber der skizzierten Lösung einer Authentifizierung des gesamten Netzes durch das Remote-Gateway kein nennenswerter Sicherheitsgewinn mehr erzielbar. Es ist daher üblicherweise zur Minimierung des Gesamtaufwands von einem solchen Ansatz eher abzuraten.

Ansatz 2: Zugriffsszenarien

Für interne Mitarbeiter empfiehlt sich in der Regel ein Zugriff über einen direkten Tunnel zwischen Client und VPN-Gateway. Diese Form des Zugriffs ermöglicht die präziseste Form der Zugriffssteuerung (s.o.) und bestmögliche Abschottung der jeweiligen Kommunikationsbeziehung von der Umgebung. Als Methode der Wahl haben sich hier in der Vergangenheit IPSec-basierte Client-to-Site-VPNs bewährt.

Aufgrund der relativen Freizügigkeit der Kommunikation, insbesondere der Möglichkeit, Daten mit dem internen Netz auszutauschen, sind an derart ausgestattete Client-Systeme gewisse Anforderungen hinsichtlich des Sicherheitsstatus zu stellen. Konkret sollte ein remote-Client systemtechnisch mindestens dem Sicherheitsstatus eines internen Clients entsprechen. Zusätzlich muss er sich über entsprechende clientseitige Firewallfunktionen gegenüber etwaigen Bedrohungen aus dem VPN-Trägernetz (also üblicherweise dem Internet) schützen können.

Es existieren VPN-Lösungen am Markt, die Mechanismen zur weitgehenden Sicherstellung eines adäquaten Client-Status bieten. Nach Möglichkeit sollte für die konkrete Realisierung einer solchen Lösung der Vorzug gegeben werden.

Produktabhängig kann alternativ der Einsatz eines SSL-basierten VPNs hierfür in Frage kommen. Dazu muss die Lösung sicherstellen, dass ein transparenter Zugang wie beschrieben nur auf der Basis eines vom Betreiber des internen Netzes gestellten Clients mit hinreichendem Sicherheitsstatus (s.o.) erfolgen kann, beispielsweise durch Einsatz eines dedizierten SSL-Clients als Lösungsbestandteil.

Es gibt jedoch auch Nutzergruppen oder Einsatzszenarien, die mit IPSec-basierten Lösungen generell nicht sinnvoll bedient werden können:

- Nicht in allen Fällen kann ein eigener Mitarbeiter einen durch seinen Arbeitgeber bzw. dessen Netzbetreiber bereitgestellten und administrierten Client („Managed PC“) für den VPN-Zugriff nutzen - nur solche kommen jedoch üblicherweise für den oben dargestellten Ansatz in Frage. Nutzt der Mitarbeiter ein „fremdes“ System, so ist mit an Sicherheit grenzender Wahrscheinlichkeit davon auszugehen, dass dieses nicht für die Nutzung des IPSec-VPN ausgestattet ist; Standard-Gründe sind fehlende Client-Software bzw. fehlendes Systemzertifikat. Sollen auch in solchen Fällen die Mitarbeiter mit einem VPN-Zugang versorgt werden, so kommt sinnvoll nur ein „clientless VPN“ auf Basis von SSL unter Nutzung eines Web-Browsers als Client in Frage. Auf dieser Basis ist ein Zugriff technisch von praktisch jedem Endgerät mit Internetzugang möglich, beispielsweise auch aus Internet-Cafés.

Aufgrund der vielfältigen Risiken für das interne Netz, die von fremden Clients ausgehen - an dieser Stelle sei exemplarisch die Verbreitung von Viren oder Würmern genannt - , kann ein solcher Zugriff allerdings nur sehr restriktiv zugelassen werden. Konkret bedeutet dies:

  - Zugriff nur Terminalserver-basiert
  - Kein Dateitransfer zwischen Client und Server

Da diese Form des Zugriffs sowohl sicherheitstechnisch als auch vom Administrationsaufwand her als optimal anzusehen ist, kann sie generell auch als Standardlösung für interne Mitarbeiter vorgesehen werden, die keinen Bedarf an transparenter Netzkopplung haben (solcher Bedarf kann z.B. aufgrund notwendiger Datenaustausche entstehen oder weil die genutzten Anwendungen nicht zur Bereitstellung via Terminalserver geeignet sind).

- Mitarbeiter von Wartungsfirmen greifen typischerweise von ihren eigenen Clients aus auf die gewarteten Systeme im internen Netz zu. Eine Installation des für einen IPSec-basierten VPN-Zugriff notwendigen VPN-Clients wirft sowohl technische als auch organisatorische Probleme auf:

  - In der Regel wird ein solcher Techniker mehr als nur einen Kunden betreuen. Die Installation mehrerer IPSec-VPN-Clients auf einem Endgerät führt jedoch in vielen Fällen zu Schwierigkeiten.

  - Es wäre zu klären, wer ggfs. für den Support solcherart ausgestatteter Clients verantwortlich ist.

  Die Bereitstellung eines entsprechenden Client-Systems durch den internen Netzbetreiber würde die beschriebenen Probleme lösen, ist aber mit Blick auf die potenziellen weiteren Kunden aus Sicht der Wartungsfirma in der Regel nicht praktikabel. Außerdem wäre ein solcher Ansatz mit zusätzlichen Kosten verbunden und die Frage des (Vor-

Ort-)Supports für diese Systeme wäre ebenfalls ein nicht trivial zu klärendes Problem.

Eine Verwendung eines clientless-Ansatzes auf Basis von SSL (s.o.) kommt ebenfalls nicht in Frage, da für solche Zugriffe aufgrund des hohen Risikopotenzials nur eingeschränkte Funktionalität vorgesehen werden sollte, die für Wartungszwecke im Allgemeinen bei weitem nicht ausreicht.

Für Zugriffe der beschriebenen Art eignet sich deutlich besser der Einsatz von Site-to-Site-Tunneln zwischen dem Netz der Wartungsfirma und dem internen Netz.

- Neben den oben angesprochenen Wartungsfirmen kommen häufig auch andere Fremdfirmen als Nutzer der VPN-Lösung in Betracht, z.B. Ingenieurbüros oder externe Berater, die in die Abwicklung von Projekten involviert sind. Für derartige Nutzergruppen reicht in den meisten Fällen ein clientless-Zugriff analog zu oben vollkommen aus.

Kann die VPN-Infrastruktur auch für sicheren Zugriff auf externe Ressourcen genutzt werden?

Neben dem klassischen Fall des Remote-Zugriffs im Rahmen der VPN-Nutzung kann auf der Basis von VPN-Technik grundsätzlich auch ein Zugriff aus dem internen Netz auf extern bereitgestellte Ressourcen erfolgen. Dies ist allerdings aus technischen Gründen nur auf Basis von Site-to-Site-VPN-Tunneln möglich.

Werden aus anderen Gründen ohnehin Site-to-Site-Szenarien durch das VPN-Konzept vorgesehen, lassen sich ohne Mehraufwand auch die beschriebenen Zugriffe realisieren.

Ist die VPN-Lösung skalierbar?

Unter Skalierbarkeit wird die Möglichkeit verstanden, eine konzipierte Lösung an unterschiedliche Mengengerüste anzupassen. Dies bedeutet, dass eine Erweiterung der Leistungsfähigkeit ohne grundsätzliche Änderungen des Konzepts möglich sein muss.

Für VPN-Lösungen sind hier vorrangig folgende Leistungsparameter relevant:

- Verschlüsselter Datendurchsatz
- Maximale Anzahl konfigurierbarer VPN-Peers (Clients oder Remote-Gateways)
- Maximale Anzahl simultan kommunizierender VPN-Peers

Grundsätzlich kommt eine Skalierung eines einzelnen VPN-Systems in der Regel nur im Bereich der unterstützten Peers in Betracht; hier lassen sich - produktabhängig - durch Speicherausbau im Rahmen der vorgesehenen Möglichkeiten entsprechende Erweiterungen der Leistungsfähigkeit realisieren. Bezüglich des Durchsatzes ist eine Skalierung nur dann möglich, wenn durch Austausch vorhandener Hardware gegen leistungsfähigere oder durch Einbau zusätzlicher Hardware der Durchsatz erhöht werden kann; dies betrifft vor allem spezielle Verschlüsselungshardware, die in allen Systemen gehobener Leistungsstufen regelmäßig verbaut wird.

Neben der systeminternen Skalierung kommt grundsätzlich auch eine externe Skalierung durch Hinzunahme weiterer VPN-Systeme hinzu; hierzu sind allerdings mehr oder weniger aufwändige Cluster-Lösungen erforderlich, die nicht nur die Kosten erhöhen, sondern darüber hinaus aufgrund der Komplexität von Loadsharing-Mechanismen im sicherheitssensiblen Verschlüsselungsumfeld nicht immer zu verbesserter Systemstabilität beitragen. Ein Verzicht auf derartige Zusatzmechanismen ist allerdings grundsätzlich möglich und im Sinne obiger Bedenken auch zu empfehlen; vorausgesetzt, eine statische Zuteilung von Peers an die unterschiedlichen VPN-Gateways ist akzeptabel.

Grundsätzlich sollte bei der Planung die Möglichkeit zukünftig steigender Bedarfe geeignet berücksichtigt werden und ggfs. bei der konkreten Produkt- bzw. Modellauswahl die Einstiegsvariante nicht zu knapp kalkuliert werden. Dann ist zumindest innerhalb eines planerisch überschaubaren Zeitraums die Notwendigkeit einer Skalierbarkeit im obigen Sinne in der Regel nicht gegeben. Muss dennoch eine Erweiterung der Leistungsfähigkeit vorgenommen werden, kann aus Kosten- sowie Praktikabilitätsgründen in den meisten Fällen ohne weiteres ein Aufbau zusätzlicher Gateways, jedoch ohne Cluster- oder Loadbalancer-Lösung erfolgen; die zu bedienenden Verbindungen werden bei diesem Ansatz im Bedarfsfalle basierend auf den bis dahin gemachten Erfahrungen statisch auf die verschiedenen Gateways aufgeteilt.

Wie sehen Maßnahmen zur Gefährdungsabwehr aus?

Jedwedes VPN-Konzept sollte auf einen möglichst sicheren Einsatz der zu schaffenden Lösung ausgelegt sein. Dabei ist vor allem den grundlegenden Sicherheitszielen entsprechend Rechnung zu tragen.

Neben den unmittelbar durch das VPN (bzw. die zu seiner Realisierung genutzten Techniken) verursachten Gefährdungen kommen zusätzlich alle bei jedweder Remote-Kommunikation anfallenden Gefährdungen in Betracht, hierzu zählen insbesondere ein Missbrauch der erteilten Zugriffsrechte durch den Anwender selbst, ein Missbrauch des VPN-Clients als Relay zum Eindringen in das interne Netz (etwa auf der Basis von so genannten Remote Access Trojanern, RAT), eine Verseu-

chung mit Viren oder ähnlichen Schadprogrammen sowie die Preisgabe interner Informationen.

Setzt man voraus, dass ein akzeptabler Grundschutz innerhalb des internen Netzes gegeben ist, der u.a. einen funktionstüchtigen Virenschutz, Sicherheitsvereinbarungen mit den internen Mitarbeitern hinsichtlich der Nutzung von IT-Ressourcen und eine sinnvolle Steuerung von Benutzerrechten umfasst - die Bereitstellung eines solchen Grundschutzes sprengt naturgemäß den Rahmen eines VPN-Projekts - , so ist den genannten Gefährdungen unter dieser Prämisse mit folgenden Maßnahmen zu begegnen:

- Sicherstellung eines funktionierenden Virenschutzes entsprechend dem Virenschutzkonzept für das interne Netz auf allen Client-Systemen, die mit dem internen Netz Daten austauschen können

  Dies impliziert:

  - Die Ausstattung aller durch den internen Netzbetreiber gestellten VPN-Clientsysteme mit einem Virenschutzmechanismus gemäß gültigem Standard

  - Nach Möglichkeit (produktabhängig) eine Überprüfung der Aktualität der jeweiligen Virendefinitionsdateien und Beschränkung der Kommunikation auf unkritische Ziele bzw. mit dem Update-Server bei Bedarf

  - Vereinbarung mit allen Fremdfirmen hinsichtlich des Einsatzes eines adäquaten Virenschutzprodukts auf deren Client-Systemen - immerhin sind diese womöglich (s.o.) per Site-to-Site-VPN mit dem internen Netz verbunden…

  - Einsatz von Virenschutzprogrammen auf allen Systemen, auf die durch externe Firmen zugegriffen wird, soweit dies technisch möglich ist - insbesondere in Produktionsbereichen und/oder bei Systemen mit Echtzeitanforderungen können sich hier leicht Probleme ergeben

- Vereinbarungen mit allen Fremdfirmen hinsichtlich der Nutzung der zum Zugriff freigegebenen Ressourcen; hierunter fällt insbesondere eine technische Beschränkung (z.B. durch einen Paketfilter) der Clients, die über das VPN auf das interne Netz zugreifen können

- Steuerung des Zugriffs interner und externer Nutzer auf interne Ressourcen durch Einsatz von Firewalltechnik (s.o.)

- Unterbindung der Kommunikation von VPN-Clients außerhalb des VPN-Tunnels (z.B. durch lokale Firewalltechnik)

- Vereinbarungen mit allen Fremdfirmen hinsichtlich deren sicherer Anbindung an weitere Netze Dritter

- Verhinderung des Datenaustauschs zwischen dem internen Netz und fremden VPN-Clients, mit deren Betreibern keine Sicherheitsvereinbarungen existieren (insbesondere Systeme in Internet-Cafés u.ä.)

Welche Standards sind bei der VPN-Kommunikation einzusetzen?

Diese Frage ist im Grunde zweigeteilt zu betrachten, nämlich hinsichtlich der technologischen Standards, denen eine Lösung sinnvollerweise folgen sollte, und hinsichtlich der organisatorischen Standards, an denen sich der Einsatz bzw. die Nutzung der Lösung zu orientieren hat.

Als technologische Standards sind hier für die beiden grundlegenden Ansätze zum einen IPSec und zu anderen HTTPS (für SSL-basierte Lösungen) zu nennen. Da beide Standards im Internet weit verbreitet sind - ja, im Grunde den Defacto-Standard repräsentieren, sollte die Forderung nach Einhaltung der Standards den Nutzern keine unangemessenen Hürden auferlegen…

In organisatorischer Hinsicht ist zwischen internen und externen Nutzern zu unterscheiden:

Interne Nutzer des VPNs müssen sich an die durch ihren „Dienstherren“ bzw. dessen Netzbetreiber festgelegten Standards halten; dies impliziert insbesondere eine entsprechende Ausstattung der VPN-Clientsysteme mit Kommunikations- und Sicherheitssoftware, soweit diese der administrativen Hoheit des besagten Netzbetreibers unterliegen.

Externe Nutzer des VPNs müssen sich an die abzuschließende (s.o.) gegenseitige Vereinbarung zur Nutzung des VPNs halten; dies sollte tunlichst mindestens die Gewährleistung eines hinreichenden Sicherheitsniveaus in Fremdnetzen beinhalten, die per Site-to-Site-Kopplung an das eigene Netz angeschlossen werden.

Welche VPN-Mechanismen kommen sinnvoll in Frage?

Aktuell kommen zwei Varianten von VPN-Mechanismen grundsätzlich in Betracht:

- IPSec
- HTTPS (SSL)

Beide Ansätze weisen prinzipbedingt sowohl Vor- als auch Nachteile auf.

- IPSec bindet VPN-Clients und Remote-Sites transparent an die zentrale Site an, d.h. - soweit nicht Einschränkungen durch zusätzliche Filterelemente vorgenommen werden - jegliche IP-basierten Kommunikationsformen werden unterstützt. Allerdings ist der Einrichtungs- und Administrationsaufwand für ein IPSec-basiertes Client-to-Site-VPN infolge der speziellen Client-Software vergleichsweise hoch.

- HTTPS-basierte VPNs (so genannte SSL-VPNs) benötigen im Prinzip keinen speziellen Client, da sie aus einem handelsüblichen Browser heraus genutzt werden. Insofern ist ein Zugriff von jedem beliebigen System aus möglich und der operative Aufwand ist vergleichsweise gering. Allerdings sind bei diesem Einsatzszenario (Nutzung von beliebigen Systemen aus) die Kommunikationsmöglichkeiten teilweise eingeschränkt. Beispielsweise wird für den technisch auch hier grundsätzlich möglichen transparenten Netzzugriff in der Regel zur Laufzeit ein Applet auf den Client geladen, zu dessen Ausführung häufig erweiterte Benutzerrechte erforderlich sind. Außerdem führt der bei diesem Konzept technisch nicht zu verhindernde Zugriff von beliebigen Systemen aus zu einem deutlich erweiterten Risikopotenzial, das sinnvoll nur durch Beschränkung auf Terminalserver-basierte Kommunikation beherrschbar ist.

In Fällen, wo sowohl der transparente Netzzugriff von Managed PCs aus als auch der (eingeschränkte) Zugriff von Fremdsystemen aus anzubieten ist, sollte das Konzept eine Kombination beider Mechanismen vorsehen (s.o.). Dabei ist es jedoch nicht zwingend erforderlich, beide Verfahren auf der Basis eines einheitlichen Produkts zu realisieren; eine diesbezügliche Diversifikation würde im Gegenteil sogar automatisch eine Redundanz bieten und damit die Verfügbarkeit der Gesamtlösung erhöhen. Allerdings steigen dabei der administrative Aufwand und die Komplexität einer redundanten LAN-Anbindung.

Wie ist mit Authentifizierung und PKI umzugehen?

Eine möglichst zuverlässige Identifizierung des jeweiligen Kommunikationspartners ist bei VPN-Lösungen unabdingbar.

Insofern sollte jedes Konzept an dieser Stelle besonderen Wert auf Einsatz als hinreichend sicher geltender Methoden zur Authentifizierung des jeweiligen Users bzw. Remote-VPN-Gateways legen.

Zur Authentifizierung von Anwendern, die von einem VPN-Client aus zugreifen, können grundsätzlich wahlweise Security-Token oder SmartCards eingesetzt werden. SmartCards kommen allerdings, wie schon dargelegt, nur dann sinnvoll in Betracht, wenn ein Zugriff von Fremdsystemen aus nicht vorgesehen ist. In entsprechend flexibel auszurichtenden Szenarien stellen daher die Security-Token nach wie vor die Methode der Wahl dar.

Die eigentliche Authentifizierung, d.h. die Überprüfung des vom Token gelieferten Passcodes auf Korrektheit, wird dabei von einem speziellen Server vorgenommen. Mit diesem Server kann das jeweilige VPN-Gateway (produktabhängig) wahlweise direkt oder über einen RADIUS-Server kommunizieren. Grundsätzlich bietet die RADIUS-basierte Variante Vorteile, da diese einen universellen Einsatz der Token-Lösung auch in anderen Bereichen grundsätzlich ermöglicht. Als RADIUS-Server kann dabei in Windows-dominierten Umgebungen prinzipiell auch ein Microsoft IAS fungieren; da in der Vergangenheit hier mitunter Kompatibilitätsprobleme auftraten, sollte dies bei Bedarf als Anforderungskriterium in einer Ausschreibung ausdrücklich formuliert werden. Über diesen Ansatz ist prinzipiell auch eine Einbindung in eine ActiveDirectory-Struktur, allerdings ist in jedem Fall derzeit noch eine separate Administration der Security Token auf dem Token-Server erforderlich (jedes Token muss in der Datenbank des Servers parametriert werden; derzeit ist dies nach Kenntnis des Autors über das AD nicht möglich).

Da für Remote-VPN-Gateways, d.h. bei Einsatz von Site-to-Site-Tunneln, eine Token-Lösung aus technischen Gründen in den allermeisten Fällen nicht eingesetzt werden kann (Ausnahme: Verwendung so genannter VPN Hardware Clients, z.B. Cisco VPN 3002), muss eine Ausweichlösung gefunden werden. Anders als bei der Authentifizierung von Anwendern kann hier - ohne erhöhtes Sicherheitsrisiko - die Verwendung zufällig generierter statischer Kennwörter ausreichender Länge (mindestens 12 Zeichen) vorgesehen werden. Schließlich muss sich bei diesem Szenario niemand diese Kennwörter merken, so dass die üblichen Gefahren der Kennwortpreisgabe nicht bestehen (sinnvoller Umgang mit der Thematik durch die jeweiligen Administratoren unterstellt…).

Wird auf eine Verwendung von SmartCards verzichtet, sind aufwändige PKI-Mechanismen nicht erforderlich. Aufgrund der technischen und insbesondere auch organisatorischen Komplexität einer sinnvollen PKI ist dies ein weiterer Vorteil der Token-basierten Lösung. Zur (zusätzlichen) Systemauthentifizierung bei IPSec sowie für den Aufbau der SSL-Kommunikationsbeziehung bei SSL-VPNs werden zwar u.U. Zertifikate benötigt, die jedoch typischerweise auf der Basis produktintegrierter Mechanismen erzeugt werden können. Demzufolge sollte das VPN-Konzept hier eine entsprechende Fähigkeit der jeweiligen Produkte vorsehen sowie optional eine Unterstützung der Windows-PKI (die Unterstützung weiterer Schnittstellen wäre in diesem Zusammenhang sicherlich wünschenswert).

Welche Schutzvorkehrungen sind bei bereichsübergreifender Kommunikation einzuplanen?

Erfolgt über die VPN-Lösung eine Kommunikation zwischen unterschiedlichen Verantwortungsbereichen, beispielsweise in Extranet-Szenarien, sind Vorkehrungen zum Schutz eigenen internen Netzes erforderlich. Hierzu wurden bereits geeignete Maßnahmen angesprochen und diskutiert:

- Beschränkung der zulässigen Kommunikation (weitestgehend vergleichbar einer Anbindung an das Internet)
- Vereinbarungen mit den jeweiligen Verantwortlichen des „fremden“ Verantwortungsbereichs

Gateway-Position, Architektur, Firewall-Integration

Da als Trägermedium für die VPN-Kommunikation das Internet genutzt wird, liegt grundsätzlich eine Positionierung des zentralen VPN-Gateways im Umfeld des in der Regel vorhandenen Internetzugangs nahe. Theoretisch kann das Gateway auch „weiter innen“ oder - im Fall größerer Netze mit mehreren per klassischer WAN-Technik verbundenen Standorten - sogar an einem anderen Standort positioniert werden. Dabei sollte man jedoch bedenken, dass dies potenziell Umwege im Pakettransport nach sich ziehen könnte, die insbesondere hinsichtlich der meist teuren und daher typischerweise hinsichtlich der Bandbreitenauslegung eher knapp kalkulierten WAN-Leitungen zwischen den Standorten vermieden werden sollten.

Hinsichtlich der Integration der VPN-Lösung in eine vorhandene Firewall-Infrastruktur existieren zwei grundlegende strategische Ansätze:

- Integration des VPN in die vorhandene Struktur
  Bei diesem Ansatz wird die VPN-Kommunikation grundsätzlich durch die Firewall(s) geschleust, wobei prinzipiell verschiedene Positionierungen des Gateways denkbar sind.
- Unabhängige Realisierung des VPN
  Bei diesem Ansatz erfolgt eine Kopplung des VPN-Gateways an die vorhandene Firewall nur bei Bedarf.

In der Praxis hat sich der zweite Ansatz als der sinnvollere erwiesen - es sei denn, es existieren entsprechend anders lautende Vorgaben, etwa im Rahmen einer übergreifenden Security Policy.

Für das Konzept empfiehlt sich auf dieser Basis typischerweise eine direkte Verbindung des VPN-Gateways mit dem Internet (Abbildung 1). Die erforderliche Steuerung der zulässigen Kommunikation innerhalb des VPN erfolgt dabei durch das VPN-Gateway. Dieser Ansatz generiert zwangsläufig Anforderungen an die Funktionalität des Gateways:

- Eine (benutzerbezogene) Filterung des VPN-Datenverkehrs muss möglich sein
- Ausreichende Schutzfunktionen gegenüber dem Internet als Trägermedium müssen zur Verfügung stehen.

Gründe für diese Empfehlung sind vor allem die nachfolgend aufgeführten:

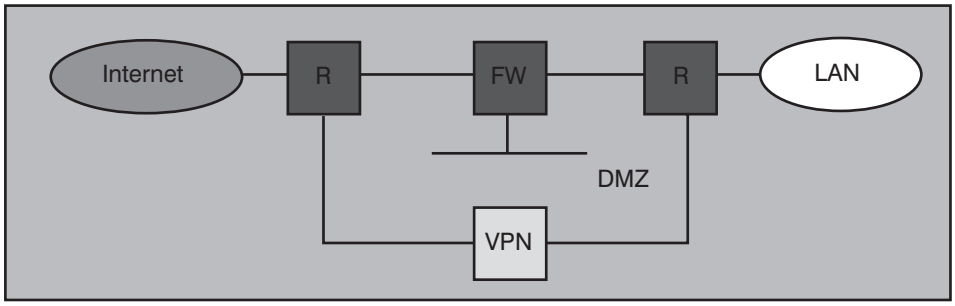


Abbildung 1: VPN-Realisierung ohne Einbindung der Firewall

- Eine Kommunikationskontrolle über eine vorhandene Internet-Firewall bedingt erhöhten Verwaltungsaufwand, da die zulässigen Kommunikationsformen benutzerabhängig zu steuern sein sollen; dazu sind aber ein entsprechendes Regelwerk und eine Korrelation zum VPN-Gateway bzw. RADIUS-Server notwendig, damit die Firewall aus dem Datenstrom den jeweiligen User ermitteln kann (z.B. über die genutzte Client-IP-Adresse). Alternativ käme eine (zusätzliche) Benutzerauthentifizierung an der Firewall in Betracht, die aber das Handling für den User erschwert und die Fehlerhäufigkeit und damit den Supportbedarf erhöht.

- Bei einem integrierten Ansatz beeinflusst die Verfügbarkeit der Firewall die des VPN; durch die Verkettung der Komponenten steigt die Fehlerwahrscheinlichkeit für das VPN an, insbesondere falls die Firewall nicht hochverfügbar ausgelegt ist.

- Der Ende-zu-Ende-Delay der über das VPN abgewickelten Kommunikationsbeziehungen steigt durch die zusätzliche Informationsverarbeitung in der Firewall an; dies kann sich auf diesbezüglich sensible Anwendungen nachteilig auswirken.

- Gleichzeitig ist der Sicherheitsgewinn einer solchen integrierten Architektur bestenfalls marginal - den Einsatz eines VPN-Gateways mit ausreichender Schutzfunktionalität vorausgesetzt. Grundsätzlich ist das Risikopotenzial eines VPN-Gateways (sofern es keinerlei sonstigen Datenverkehr bedienen muss) deutlich geringer als das einer Firewall. Dies liegt daran, dass die zulässigen Pakete aus Sicht eines VPN-Gateways meist erheblich stärker - zumindest jedoch in gleichem Maße wie durch eine vorgeschaltete Firewall (Abbildung 2 zeigt eine beliebte Architekturvariante) - eingeschränkt werden können.

  Für eine Lösung mit IPSec und SSL-VPN werden nur die Protokolle IKE (UDP500 und ggfs. UDP4500), HTTPS (TCP443) und ESP (IP50) benötigt; alle übrigen Datenpakete können prinzipiell verworfen werden. Hinzu kommt, dass zumindest bei IPSec weitere Mechanismen wie z.B. die Systemauthentifizierung zum Einsatz kommen, die den Missbrauch der zulässigen Protokolle durch Fremde bei sorgfältiger Konfiguration praktisch ausschließen.

Die zusätzliche Verwendung von Firewalls bei der Anbindung des VPN-Gateways ließe sich somit lediglich mit einer ggfs. notwendigen zentralen Steuerungsfunktion begründen - etwa wenn über eine solche Firewall die Kommunikation von ebenfalls auf dem Campus ansässigen Fremdfirmen von den eigenen Datenströmen getrennt werden muss. Aus Sicht der möglichst frühzeitigen Auskopplung derartiger mehr oder minder unkontrollierbarer Kommunikationsströme ist in solchen Fällen eine entsprechende Anbindung an die besagte Firewall sinnvoll (Abbildung 3). Die Steuerung des sonstigen VPN-Verkehrs hingegen kann von einem geeigneten VPN-Gateway deutlich besser und mit weniger Administrationsaufwand wahrgenommen werden (s.o.).

Welche VPN-Komponenten werden benötigt?

Rein funktional kann ein VPN Gateway-seitig wahlweise auf Basis einer Appliance oder einer Software-Lösung realisiert werden. Erfahrungsgemäß neigen allerdings Appliances zu insgesamt stabileren Betriebsresultaten und reduzieren in Summe den operativen Aufwand.

Client-seitig ist in den allermeisten Fällen eine Software-Lösung vorzusehen. Üblicherweise bietet der Hersteller des VPN-Gateways eine passende Client-Komponente mit an. Theoretisch kann auch ein alternativer Client eingesetzt werden; dies führt jedoch in der Praxis häufig zu technischen Schwierigkeiten und sollte daher nur in Verbindung mit ausgiebigen Tests erwogen werden. Hinzu kommt, dass proprietäre Zusatzmechanismen (z.B. in den Bereichen Benutzer-Authentifizierung, Client-Update, Client-Policy, etc.) in aller Regel nur auf Basis einer homogenen Lösung nutzbar sind.

Es sind auch so genannte Hardware-Clients am Markt verfügbar (s.o.); eine Festlegung auf einen solchen Ansatz würde jedoch die Produktauswahl stark einschränken. Zudem kommen solche Systeme aus Gründen der Praktikabilität nur sinnvoll bei stationären Clients in Betracht - es wäre dem Anwender sicher-

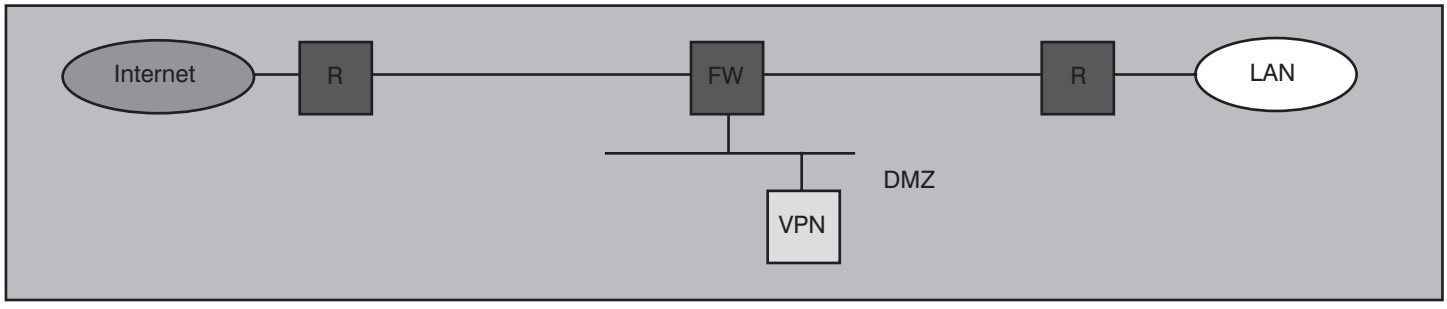


Abbildung 2: VPN-Realisierung mit vor- (und nach-)geschalteter Firewall

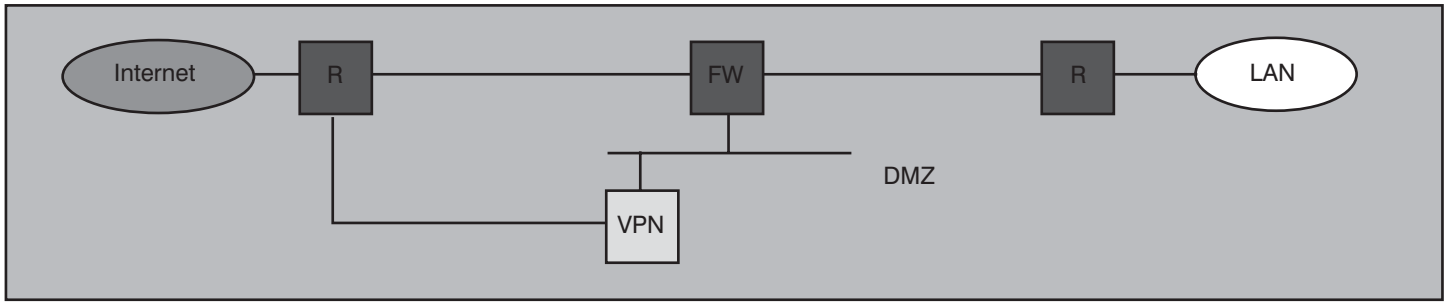


Abbildung 3: VPN-Realisierung mit Filterung der entschlüsselten Datenströme

lich kaum zu vermitteln, dass sein neues Notebook zwar erneut kleiner und leichter als das alte ausfallen wird, er jedoch zum Ausgleich ein weiteres Gerät inklusive Netzteil etc. zwecks VPN-Nutzung bei sich tragen muss...

Sollte bei der Auswahl einer Lösung die Entscheidung für einen Hersteller fallen, der derartige Hardware-Clients im Portfolio hat, könnten diese jedoch durchaus eine Alternative für die Realisierung von Site-to-Site-Kopplungen darstellen.

Auf die Anordnung der Komponenten wurde bereits eingegangen. Zur Authentifizierung sind zusätzlich weitere Komponenten, typischerweise ein RADIUS-Server und ein Token-Server vorgesehen. Diese können prinzipiell an beliebiger Stelle im internen Netz positioniert sein, wobei etwaige Empfehlungen der jeweiligen Hersteller zum Schutz dieser Server zu beachten sind; eine Positionierung in einem besonders geschützten Netzsegment ist unter Sicherheitsaspekten sicherlich zu bevorzugen.

Es ist von Vorteil, wenn das VPN-Gateway auf einer speziell gehärteten Firmware bzw. OS-Plattform basiert. Vor diesem Hintergrund ist Lösungen, die eine eigene geeignete Firmware bzw. OS bereits mitliefern, gegenüber Lösungen, die auf einer Standard-Plattform aufsetzen, der Vorzug zu geben.

VPN-Client-Software sollte über eine geeignete lokale Firewall-Funktionalität zum Schutz des Clientsystems gegen das VPN-Trägermedium verfügen. Als Mindestanforderung gilt eine Möglichkeit, einen so genannten „Split Tunnel“, d.h. die Möglichkeit gleichzeitig mit dem Internet und per VPN mit dem internen Netz zu kommunizieren, administrativ zu unterbinden. Alle Schutzfunktionen („Client-Policy“) sollten zentral administrierbar sein. Andernfalls ist ein nicht unerheblicher Pflegeaufwand, je nach Größe der Nutzerpopulation, zu kalkulieren. Bietet die Software zusätzlich eine Prüfung des Client-Status (etwa hinsichtlich des Relase-Stands der VPN-Software oder des Virenschutzes, s.o.), so ist dies eindeutig positiv zu bewerten, da es die verbleibenden Restrisiken der VPN-Nutzung deutlich reduziert.

Welche grundlegenden Konfigurationsvorgaben sind zu machen?

Allgemein sollte die Regel „Sicherheit vor Funktionalität“ gelten. Das bedeutet, dass alle Komponenten des VPN so zu konfigurieren sind, dass ein als hinreichend betrachtetes Sicherheitsniveau erreicht wird - notfalls unter Verzicht auf bestimmte nicht unbedingt notwendige Funktionalitäten. Diesem Grundsatz sollte das gesamte Konzept Rechnung tragen, als Beispiel wären hier die zuvor empfohlenen Beschränkungen bei SSL-VPNs zu nennen.

Über diese konzeptionellen Aspekte hinaus sind alle Systeme mindestens entsprechend dem im jeweiligen internen Netz etablierten Sicherheitsstandard zu konfigurieren; ggfs. kann eine Orientierung an den Vorgaben des Grundschutzkatalogs des BSI erfolgen. Zu den Standardmaßnahmen zählen hier:

- Beschränkung des administrativen Zugriffs auf das verantwortliche Personal
- Deaktivierung von Default-Konten; Einrichtung spezifischer Administratorkonten
- Verwendung hinreichend starker Kennwörter - alternativ kann eine zur Authentifizierung der VPN-Anwender eingesetzte Token-Lösung auch für die Administration der VPN-Komponenten verwendet werden.

Analog ist hinsichtlich der Backup- und Recovery-Thematik zu verfahren.

Wie können Redundanzen geschaffen werden?

Für VPNs sind verschiedene Redundanz-Mechanismen realisierbar. Ergibt sich auf Basis der Ist- und Anforderungsanalyse keine zwingende Notwendigkeit für eine automatisch aktiv werdende Redundanzlösung, so kann beispielsweise schon die Bevorratung eines zum primären zentralen VPN-Gateway identisch konfigurierten sekundären Gateways als prinzipiell ausreichend angesehen werden.

Soll das auszuwählende Produkt andererseits jedoch eine entsprechende Option aufweisen, empfiehlt sich - ja nach konkreter Lösung - die Nutzung entsprechender Failover- Mechanismen, soweit diese ohne nennenswerten Mehraufwand realisierbar sind. Dies ist bei diversen Produkten der Fall.

Externe Lösungen (z.B. Load-Balancer) allein können in der Regel ein automatisiertes Failover oder gar eine Lastverteilung nicht bewerkstelligen (zumindest im Fall von IPSec-basierten VPNs). Insofern ist praktisch immer eine entsprechende Funktionalität innerhalb des VPN-Produkts vonnöten. Damit ergibt sich unmittelbar, dass Redundanz- bzw. Lastverteilungsmöglichkeiten stark produktabhängig sind - allgemeine konzeptionelle Vorgaben ohne Produktbezug sind daher kaum möglich.

Soll bzw. muss die Beschaffung der Lösung auf dem Ausschreibungswege erfolgen, so sind entsprechende funktionale Optionen produktneutral in die Leistungsbeschreibung aufzunehmen, damit die Produktauswahl entsprechende potenzielle Anforderungen berücksichtigen kann. Ähnliches gilt für die Authentifizierungslösung: auch hier sind die jeweiligen Möglichkeiten produktabhängig und sollten über entsprechende funktionale Anforderungen im Rahmen der Ausschreibung sichergestellt werden.

Was ist bei der Migration zu berücksichtigen?

Im Zuge der Migration auf die konzipierte VPN-Lösung sind folgende Aktivitäten notwendig:

- Inbetriebnahme der VPN-Lösung einschließlich aller flankierenden Systeme (z.B. Token-Server, Terminalserver für SSL-VPN, etc.)
- Festlegung der zukünftigen Nutzerkreise

  Achtung: der Umstieg von klassischen RAS-Lösungen auf eine VPN-basierte Zugriffsform kann gewisse potenziell unerwünschte Nebenwirkungen mit sich bringen. So können beispielsweise bei einer Dial-In-basierten RAS-Nutzung mit Hilfe des Callback-Verfahrens die Zugriffskosten zentral übernommen werden; diese Möglichkeit der Kostenübernahme ist bei einer VPN-gestützten Lösung nicht gegeben. Derartige Auswirkungen sind bei der Entscheidung, welche Nutzer migriert werden, ggfs. zu berücksichtigen.
- Erstellung von Prozessbeschreibungen für die mit der VPN-Lösung verbundenen administrativen Vorgänge (z.B.: Ausstellung Token, Anlegen VPN-Nutzer, etc.)
- Erstellung von Richtlinien für die Nutzer; dazu zählen insbesondere die notwendigen Aspekte von Vereinbarungen mit Fremdfirmen
- Erstellung eines Vorschlags für ein Rollen- und Berechtigungskonzept für die Nutzung des VPN
- Einrichtung der Nutzer und Nutzergruppen und ihrer Zugriffsrechte
- Installation der IPSec-Client-Software auf den Managed PCs und Vergabe der jeweiligen Security Tokens
- Bei Bedarf: Schulung der Anwender
- Bei Bedarf: Sukzessive Deaktivierung der Dial-In-Accounts bereits auf VPN migrierter Nutzer
- Planung und Einrichtung der Site-to-Site-VPN-Verbindungen (hierfür wird je Fall die Aufstellung eines gesonderten Migrationsplans empfohlen)
- Sukzessive Deaktivierung der Dial-In-Accounts bereits auf VPN migrierter Remote Sites
- Abbau aller vollständig abgelösten Dial-In-Lösungen nach Ablauf einer festzulegenden Übergangsfrist

Bei einigen der aufgezählten Aktivitäten kann es sinnvoll sein, diese als Leistung vom Lieferanten der VPN-Lösung einzufordern. Dies gilt insbesondere dann, wenn ein starker Produktbezug gegeben ist, etwa bei der Aufstellung der Prozessbeschreibungen.

Welche Vorgaben sind für Clients zu spezifizieren?

Die Vorgaben für die Ausstattung der VPN-Teilnehmer mit Sicherheitsfunktionalitäten hängen nicht zuletzt von der jeweiligen Sicherheitspolitik und dem darauf basierenden Sicherheitskonzept ab. Im Folgenden werden wir daher lediglich einige grundlegende empfehlenswerte Maßnahmen betrachten, die speziell bei Nutzung VPN-basierter Remote-Zugriffe zu berücksichtigen sind.

- Managed PCs

  Managed PCs erhalten in jedem Fall zusätzlich zu ihrer Standard-Ausstattung eine Personal/Desktop Firewall-Funktionalität. Diese dient dem Schutz sowohl des Clients als auch des internen Netzes gegenüber dem Internet (u.a. durch Verhinderung so genannter Split Tunnels).

  Idealerweise sollte diese Funktionalität Bestandteil der VPN-Client-Software sein. In diesem Fall wird keine zusätzliche Software benötigt, und es kann von einem optimalen Zusammenspiel von IPSec-Client und Desktop Firewall ausgegangen werden. Die meisten für den Enterprise-Einsatz ausgelegten Produkte bieten darüber hinaus ein zentrales Management der Policies dieser Firewalls. Auf diese Weise lässt sich eine einheitliche Sicherheitsstrategie besonders effizient umsetzen.

  Der Einsatz von Intrusion Detection oder Sicherheitsagenten ist prinzipiell möglich, sollte aber nicht zuletzt aus Kostengründen nicht zur generellen Vorgabe gemacht werden. Bei hinreichend restriktiver, d.h. sicherer Firewall-Policy ist das Risiko eines netzbasierten Einbruchs als gering einzustufen. Sicherheitsagenten können erwogen werden, um einen adäquaten Sicherheitsstaus des Clients auch hinsichtlich installierter Software, eventuellen Virenbefalls, Aktualität des Virenscanners etc. sicherzustellen. Allerdings sind derartige Funktionen je nach Produkt teilweise bereits Bestandteil der VPN-Lösung. Daher sollte hier eine Entscheidung frühestens nach Auswahl eines konkreten Produkts getroffen werden.
- Fremd-PCs im Rahmen von Site-to-Site-Zugriffen

  Vorgaben für derartige Fremd-PCs können in der Regel nur in geringem Umfang gemacht werden.

  Im Rahmen des Konzepts sollte jedoch, wie schon angesprochen, mindestens der Einsatz eines hinreichend aktuellen Virenschutzes verlangt werden. Darüber hinaus sollte im Rahmen gegenseitiger Vereinbarungen auf weitergehende Maßnahmen gedrungen werden, die zumindest einen akzeptablen Grundschutz der jeweiligen Client-Systeme gewährleisten.
- Fremd-PCs im Rahmen von SSL-VPN-Zugriffen

  Da derartige Zugriffe von beliebigen Systemen aus technisch möglich und in der Regel auch gewollt sind (Stichwort: Flexibilität), sind hier keinerlei Vorgaben möglich. Das Konzept sollte dies durch die strikte Beschränkung derartiger Zugriffe auf per Terminalserver bereitgestellte Applikationen ohne Möglichkeit zum Datentransfer berücksichtigen.

  Es existieren auch SSL-VPN-Lösungen, die eine Remote-Überprüfung des jeweiligen Clients durch das Gateway ermöglichen sollen. Der ggfs. eingeschränkte Zugriff wird dabei vom Ergebnis dieser Überprüfung abhängig gemacht. Hier waren die Produkte aber nach Ansicht des Autors in der jüngeren Vergangenheit noch nicht so ausgereift, dass man diese Strategie grundsätzlich empfehlen könnte. Je nach Funktionalität des ins Auge gefassten konkreten Produkts kann dies im Einzelfall jedoch eine Alternative darstellen; bei erfolgreichem Verlauf entsprechender Tests kann in solchen Fällen von der Beschränkung auf Terminalserver eventuell abgesehen werden.

Welche organisatorischen Maßnahmen sind zur Einführung des VPN nötig?

Da durch Umstieg auf VPN-Technologie - sorgfältige Planung und Umsetzung unterstellt - keine zusätzlichen Gefahrenpotenziale gegenüber klassischen Lösungen (Dial-In) entstehen, sind im Grunde keine weiter gehenden organisatorischen Maßnahmen vonnöten. Dabei wird unterstellt, dass eine vorhandene Dial-In-Lösung die-

sen Gefahrenpotenzialen bereits durch entsprechende technische Maßnahmen begegnet.

Ist dies nicht der Fall oder sieht das Konzept die Einführung zusätzlicher - bisher nicht vorhandener - Schutzmechanismen vor, so sind für deren sinnvollen und effizienten Einsatz die notwendigen organisatorischen Strukturen zu schaffen.

Dies betrifft häufig vor allem den Einsatz von Security Token zur starken Authentifizierung, da viele bestehende Dial-Szenarien auf Basis herkömmlicher Kennwort-Authentifizierung realisiert wurden. Neben der Benennung des verantwortlichen Systemadministrators bedarf es hier vor allem der Etablierung eines Verfahrens zur Beantragung, ggfs. Generierung und Zuteilung der Token und der benutzerbezogenen, geheimen PIN.

Von der Theorie zur Praxis:
Ein beispielhaftes Projekt

Im Folgenden soll kurz ein reales Projekt beispielhaft dargestellt werden, das auf Basis der vorstehenden grundsätzlichen konzeptionellen Überlegungen und Empfehlungen realisiert wurde.

Ausgangslage war ein MAN basiertes Netz, das unterschiedliche technische Lösungen (u.a. Internet-basierte VPNs sowie verschiedene Dial-In- und Dial-Out-Konstrukte) für den Remote-Zugriff auf interne Ressourcen bzw. den Zugriff aus dem Intranet auf externe Ressourcen nutzte. Diese Vielfalt sollte im Sinne einer weitgehenden Harmonisierung durch eine möglichst einheitliche Lösung auf VPN-Basis abgelöst werden. Insofern musste die zu schaffende Lösung sowohl hinreichend flexibel sein als auch geeignete Skalierungsoptionen bieten. Dabei wurde die Lösung so gestaltet, dass sie unter Abwägung von Sicherheitsanforderungen, Praktikabilität und Kostenaspekten weitgehend optimal ist. Insbesondere die beiden letzten Aspekte bedingten wie so oft auch in diesem Fall punktuell Kompromisse hinsichtlich der Sicherheitsmaßnahmen; die gefundene Lösung konnte aber auf der Basis von „Best Current Practice"-Lösungen sicherstellen, dass das zu tragende Restrisiko überschaubar und insbesondere deutlich geringer war als auf Basis des Status Quo.

Als technischer Lösungsansatz für das VPN wurde der Einsatz dedizierter VPN-Appliances als VPN-Gateways vorgesehen, die sowohl Clients als auch Remote-Standorte über einen stark verschlüsselten VPN-Tunnel an das interne Netz anbinden können.

Für den Aufbau der VPN-Tunnel wurden die beiden Standard-Mechanismen

- IPSec
- SSL (HTTPS)

vorgesehen, um eine möglichst breite Palette von remote-Systemen unterstützen zu können. Aus Gründen der einheitlichen Administration und der einfacheren Architektur wurden dabei Lösungen bevorzugt, die beide Techniken innerhalb einer gemeinsamen Plattform anbieten.

Da bei SSL-VPNs im Allgemeinen von einem sehr hohen Gefährdungspotenzial durch den zugreifenden Client ausgegangen werden muss, wurde bei dieser Zugriffsform die Kommunikation auf die Nutzung von Applikationen auf Terminalserver-Basis beschränkt. Insbesondere wurde jeglicher Dateitransfer zwischen Client und internem Netz unterbunden – eine Funktionalität, die mit Blick auf die geforderte Flexibilität der Lösung dennoch durch die Implementierung nicht grundsätzlich ausgeschlossen wird.

IPSec-Clients und Clients aus Remote-Sites greifen über transparenten IPSec-Tunnel auf das interne Netz zu. Innerhalb dieses Tunnels wird die zulässige Kommunikation durch Einsatz von Firewall-Technik gesteuert. Diese Steuerung wird insbesondere zur Trennung der unterschiedlichen Nutzerkreise

- Eigene Mitarbeiter,
- Wartungsfirmen bzw. Kunden sowie
- Ingenieurbüros, die an der Neugestaltung der Liegenschaften arbeiten,

eingesetzt.

Das Konzept sah nicht zwingend eine hochverfügbare Ausrichtung der Lösung vor, da seitens des Auftraggebers ein Cold-Standby-Ansatz als ausreichend angesehen wurde. Soweit jedoch im Rahmen der Realisierung Produkte zum Einsatz kämen, die ohne Mehrkosten mindestens einen Hot-Standby realisieren könnten, sollte diese Option auch genutzt werden.

Im Folgenden wird daher der Begriff „VPN-Gateway" synonym sowohl für ein einzelnes System als auch für ein entsprechendes Cluster gebraucht.

Über ein solches Cluster ließ sich auch - wiederum produktabhängig - eine Skalierung der Lösung durch Hinzunahme weiterer Gateways mit Lastverteilung erreichen.

Aus architektonischer Sicht war vorgesehen, das VPN-Gateway in die bestehende Firewall-Architektur am zentralen Standort zu integrieren. Dazu wurde sein externes Interface mit einem internen Interface der äußeren Firewall und sein internes Interface mit dem externen Interface der inneren Firewall verbunden (Abbildung 4).

Durch diese Architektur wird das VPN-Gateway gegenüber dem Internet durch die vorhandene Firewalltechnik geschützt.

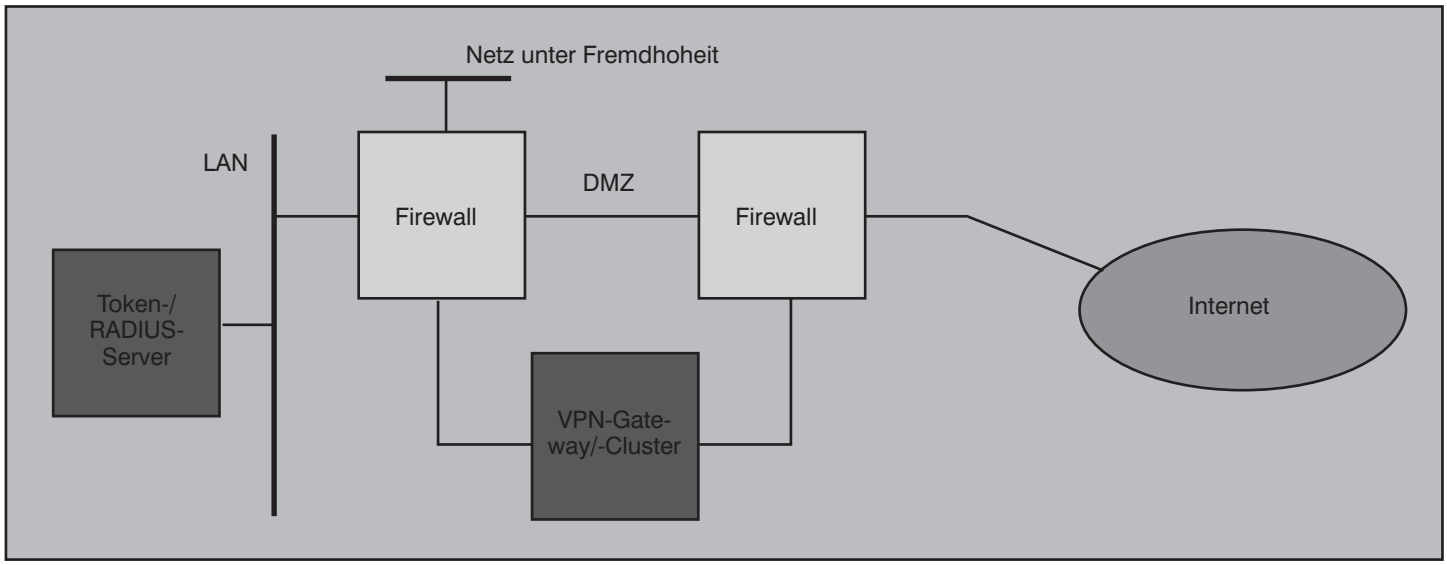


Abbildung 4: VPN-Architektur; Integration in Firewall-Architektur

Es ist jedoch eine direkte Verbindung des VPN-Gateways mit dem Internet nicht zwingend ausgeschlossen; eine derartige Architektur könnte zu einem späteren Zeitpunkt problemlos realisiert werden (Abbildung 5). Gleichzeitig erlaubt die Architektur eine Auskopplung jenes VPN-internen Datenverkehrs, der für - über die interne Firewall angebundene - Netze unter Fremdhoheit bestimmt ist. Eine weitergehende Filterung des VPN-Verkehrs durch die interne Firewall wurde nicht vorgesehen; diese erfolgt durch das VPN-Gateway.

Das Gateway musste zur sicheren Realisierung dieses Ansatzes mindestens folgende Eigenschaften aufweisen:

- Ausreichender Eigenschutz (durch Paketfilter o.ä.) gegen Gefahren aus dem Internet
- Benutzerbezogene Filterung des VPN-Datenstroms zur Steuerung der VPN-internen Kommunikation

Die Authentifizierung der Remote-User ist, wie schon angesprochen, eine der wesentlichsten Aufgaben einer sicheren RAS-Lösung - unabhängig davon, ob per Dial-In oder per VPN. Demzufolge wurde hier mit dem Einsatz einer Token-basierten Zwei-Faktoren-Authentifizierung eine besonders sichere Lösung konzipiert.

Aus Gründen der Flexibilität sollte die Anbindung dieser Authentifizierungslösung an das VPN-Gateway über einen vorgeschalteten RADIUS-Server erfolgen (der allerdings in aller Regel auf demselben System wie der Token-Server arbeitet). Dieser sollte gleichzeitig auch die Authentifizierung der Remote-Sites übernehmen, die typischerweise nur über Passwörter erfolgen kann; allerdings können diese so lang und komplex gewählt werden, dass hierdurch kein Sicherheitsrisiko entsteht.

Zusätzlich zur Authentifizierung der Nutzer erfolgt eine Identifizierung der Clients interner Mitarbeiter, z.B. zertifikatsbasiert.

Die Verwaltung der Benutzer ist aus technischer Sicht bei dem vorgelegten Konzept eine Verwaltung der Security-Token: je ein Token ist je einem Benutzer fest zugeordnet, und aus Sicht des VPN sind der Benutzer und sein Token identisch. Die Verwaltung der so definierten „Benutzer“ erfolgt damit zwangsläufig durch den Token-Server in einer speziellen Datenbank.

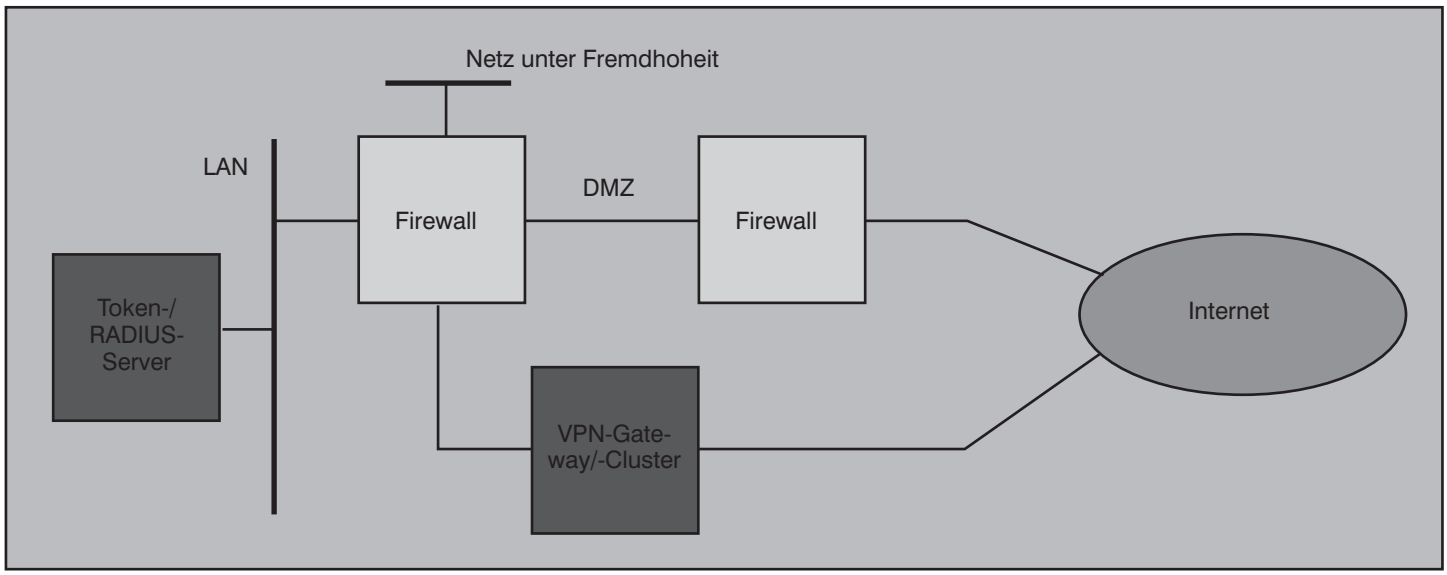


Abbildung 5: VPN-Architektur; unabhängig von Firewall-Architektur

Report des Monats

VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung

Der komplett überarbeitete und neu aufgelegte Technologie-Report von ComConsult Research zeigt alle wichtigen Meilensteine bei Aufbau, Organisation und Betrieb einer VPN-Lösung. Die einzelnen Bausteine typischer Installationen werden anhand praxisnaher Vorgaben bewertet und ein umfangreiches Projekt- und Konfigurationsbeispiel detailliert besprochen. Insgesamt werden Sie somit in die Lage versetzt, Ihre eigene technisch und wirtschaftlich optimale VPN-Lösung zu entwerfen, in Ihr Gesamtkonzept einzubinden und zu betreiben. Lesen Sie im Folgenden einen Ausschnitt aus dieser Studie.

1.1 IPSec und das NAT-Problem

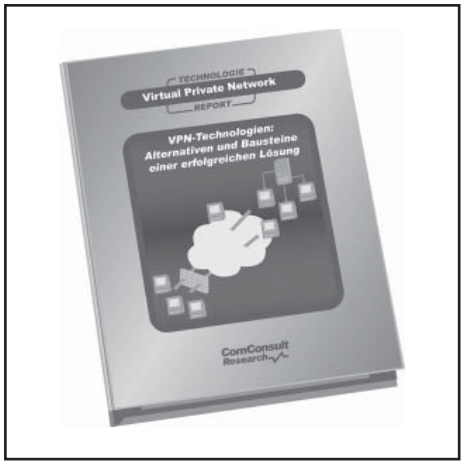
Der heute weit verbreitete Einsatz von NAT – hervorgerufen durch die Notwendigkeit, den knappen IPv4-Adressraum optimal zu nutzen, sowie aufgrund sicherheitstechnischer Vorteile bestimmter NAT-Varianten - hat beim Einsatz von VPN-Lösungen in der Vergangenheit meist für Probleme gesorgt, die erst seit Anfang 2005 durch standardisierte Mechanismen zumindest größtenteils behoben werden können. Dieses Kapitel behandelt Ursachen und Lösungsansätze dieses NAT-Problems.

1.1.1 Das NAT-Problem

Diverse Mechanismen von IPSec und NAT vertragen sich nicht miteinander. Insofern handelt es sich eigentlich nicht um ein NAT-Problem sondern um diverse NAT-Probleme. Wir wollen im Folgenden sukzessive diese Problembereiche untersuchen und beginnen bei dem offensichtlichen: dem Authentication Header.

Authentication Header

Der Authentication Header (AH) generiert eine kryptografische Prüfsumme über den Inhalt des IPSec-Pakets in Form eines Hashwerts, zu dessen Berechnung ein geheimer symmetrischer Schlüssel erforderlich ist. Dieser Hashwert umfasst alle im Paket befindlichen Daten mit Ausnahme des AH-Prüfsummenfelds und der nicht-statischen Informationen des IP-Headers. Da der Hashwert ohne Kenntnis des Schlüssels nicht gezielt gefälscht und der Schlüssel seinerseits aufgrund der Eigenschaften der Hash-Funktion nicht aus dem Hashwert zurückberechnet werden kann, wird jegliche Manipulation am Datenpaket



bei der Verifikation der Prüfsumme aufgedeckt und ein solches Paket vom Empfänger als ungültig verworfen. Der AH dient somit dem Erhalt der Integrität der übertragenen Datenpakete.

Unglücklicherweise basiert jedoch der NAT-Mechanismus bekanntermaßen genau auf einer gezielten Manipulation der IP-Adressen der Datenpakete: In der Regel wird die Absenderadresse durch eine andere Adresse ersetzt. Diese Manipulation wird vom AH äußerst wirksam unterbunden – er kann an dieser Stelle nicht zwischen erwünschten (NAT) und unerwünschten (IP-Spoofing) Manipulationen unterscheiden. Ein Einsatz des AH in NAT-Szenarien ist somit ausgeschlossen.

ESP und NAPT/PAT

Dies allein scheint nicht weiter dramatisch, wird doch der AH in vielen Szenarien gar nicht verwendet bzw. kann meist darauf verzichtet werden, da das zweite IPSec-Protokoll, ESP, ebenfalls eine - wenn auch nicht ganz so weit reichende - Integritätsprüfung beinhaltet. Doch leider löst auch der Verzicht auf den Authentication Header das NAT-Problem nicht, denn auch ESP (Encapsulating Security Payload) verursacht Probleme im Zusammenspiel mit NAT. Ein generelles Problem sind hier gemultiplexte NAT-Kommunikationsbeziehungen.

Multiplexing ist bei NAT dann vonnöten, wenn mehrere interne Adressen auf eine (oder wenige) externe Adresse abgebildet werden müssen - das Standard-Szenario etwa bei der Verwendung von DSL-Routern im SOHO-Bereich. Üblicherweise kommt hier NAPT (Network Address and Port Translation) zum Einsatz - dieser Mechanismus ist auch unter der Bezeichnung PAT (Port Address Translation) bekannt. NAPT/PAT multiplexen durch gezielte Manipulation des Client-Ports (bei UDP bzw. TCP) oder anderer aus Sicht des Empfängers frei wählbarer Parameter (z.B. ICMP-Identifier). Durch eine eindeutige Zuordnung der jeweiligen internen Adresse zu einem solchen Parameter lassen sich die Antwortpakete gezielt demultiplexen.

Unglücklicherweise verschlüsselt ESP den Teil des IP-Pakets, in dem sich diese manipulierbaren Parameter befinden. Somit ist eine sinnvolle Manipulation nicht mehr möglich und das Verfahren scheitert. Einzige Chance - für entsprechend ausgestattete NAT-Geräte - wäre eine Nutzung des IPSec-Headers zum Multiplexen. Hier steht allerdings lediglich der SPI (Security Parameter Index) zur Verfügung, der wegen der in ESP integrierten Integritätsprüfung nicht manipulierbar ist. Freilich bestünde grundsätzlich die Möglichkeit, den originalen ISP zu verwenden - immerhin ist die Wahrscheinlichkeit einer Kollision aufgrund der 32 Bit Länge des SPI extrem unwahrscheinlich - allerdings besteht hier ein grundsätzliches Problem: der SPI wird für jede der beiden Kommunikationsrichtungen zwischen den beteiligten Partnern separat vereinbart. Die Folge davon ist, dass zwischen dem SPI der gesendeten Pakete und dem der empfangenen nicht notwendigerweise eine Korrelation besteht. Anders ausgedrückt: der Empfänger eines Antwortpakets kann aus dem darin enthaltenen SPI nicht mit Sicherheit die korrekte Adressabbildung ermitteln, da dieser SPI mit dem zuvor gesendeten in keinem erkennbaren Zusammenhang stehen muss.

Daher ist diese Methode nicht allgemein verwendbar; es gibt allerdings Produkte (beispielsweise von Cisco Systems), die in der Lage sind, identische SPIs auf beiden Seiten der Kommunikationsbeziehung sicherzustellen, und somit ein NAPT/PAT ermöglichen, solange die VPN-Lösung homogen bleibt.

ESP im Transport-Modus
Es bliebe somit - wenn überhaupt - nur statisches NAT, d.h. die feste Zuordnung externer zu internen Adressen - ein Ansatz, der in den meisten Fällen an zu knapp bemessenem offiziellem Adressraum scheitern dürfte. Zudem ist auch der Einsatz von statischem NAT nicht unproblematisch: Schwierigkeiten treten zumindest dann auf, wenn ESP im Transport-Modus verwendet wird (dies ist beispielsweise bei der in Windows2000/2003 integrierten IPSec-VPN-Lösung der Fall). Ursächlich hierfür ist der Prüfsummenmechanismus in TCP (teilweise auch in UDP), der neben den Source- und Destination-Ports auch die jeweiligen IP-Adressen von Sender und Empfänger berücksichtigt. Ändert ein NAT-Gerät eine IP-Adresse, so muss der TCP-Header, konkret: das Prüfsummenfeld, entsprechend angepasst werden. Ohne ESP stellt dies kein Problem dar, mit ESP jedoch sehr wohl, da das Prüfsummenfeld verschlüsselt ist. Eine Korrektur ist somit nicht möglich – sie würde von der Integritätsprüfung von ESP sofort entdeckt werden – was dazu führt, dass die Prüfsummenverifikation beim Empfänger scheitert und dieser derartige Pakete verwirft.

Dieses Problem tritt allerdings nur im Transport-Modus auf: Im Tunnel-Modus bezieht sich die TCP-Prüfsumme auf den inneren IP-Header, während die Manipulation am äußeren, dem Tunnel-IP-Header vorgenommen wird. Da dieser auch von der ESP-Integritätsprüfung nicht erfasst wird, kann in diesem Fall statisches NAT eingesetzt werden.

IKE
Somit bliebe also ESP im Tunnel-Modus mit statischem NAT als mögliche Verfahrensweise, die in diversen DSL-Routern im Übrigen unter der Bezeichnung „IPSec-Pass-Through“ implementiert ist. Unglücklicherweise hat jedoch auch IKE Probleme mit NAT; hierfür gibt es gleich mehrere mögliche Ursachen:

- IKE verwendet, abhängig von Einsatzform und Implementierung, IP-Adressen zur Identifizierung der Kommunikationspartner. Diese befinden sich als Parameter innerhalb des IKE-Protokolls. Stimmen diese Parameter mit den tatsächlichen IP-Adressen nicht überein, so wird ein entsprechendes Paket meistens verworfen.

- IKE verwendet selbst ebenfalls SAs, um einen geschützten Kommunikationspfad („IKE-Tunnel“) für das Aushandeln der IPSec-SAs bereitzustellen. Die zugehörigen IKE-SAs bestehen in aller Regel recht lange, um beispielsweise ein regelmäßiges Rekeying (dabei werden in bestimmten Zeitabständen die Schlüssel für die ESP-Verschlüsselung neu vereinbart) mit größtmöglicher Effizienz zu gestalten. Demgegenüber sind die NAT-Timeouts für UDP, dem von IKE genutzten Transportschicht-Protokoll, in der Regel erheblich kürzer. Da über IKE nur bei Bedarf Informationen ausgetauscht werden, kommt es häufig zu langen Idle-Perioden, die dazu führen, dass das Adress-Mapping aus der NAT-Table gelöscht wird, was zur Unzustellbarkeit der betroffenen IKE-Pakete führt.

- Nicht alle IKE-Implementierungen akzeptieren Client-Ports, die vom Standard-Port (UDP 500) abweichen. Verändert ein NAT-Gerät den Source-Port eines abgehenden Pakets und der Empfänger akzeptiert nur den Port 500, so kommt keine Kommunikation zustande - die Aushandlung des IKE- und damit auch des IPSec-Tunnels scheitert.

Somit verbleibt oftmals nur die manuelle SA-Konfiguration, wenn NAT im Einsatz ist - ein Ansatz, der zumindest in umfangreicheren Szenarien absolut nicht praktikabel ist.

Lösungsansatz: Encapsulation
Das grundlegende Problem wurde natürlich schon vor geraumer Zeit erkannt und es existieren diverse Lösungen dafür, die jedoch allesamt proprietärer Natur sind. Allen derartigen Techniken ist gemeinsam, dass sie Encapsulation als Lösungsansatz verwenden, was nahe liegt, da sich damit - man sieht es beim ESP-Tunnel-Modus - einige Probleme quasi von selbst lösen.

Die meisten Hersteller generieren einen zusätzlichen UDP-Tunnel unter Verwendung verschiedenster Portnummern; eine etwas ausgefallenere Lösung bot die (mittlerweile strategisch durch die XSR-Router ersetzte) Aurorean-VPN-Lösung der Fa. Enterasys: Hier kam eine Verkapselung in HTTPS zum Einsatz, in der Hoffnung, auf dieser Basis aus vielen Netzwerken heraus ohne Anpassung einer etwaigen Firewall per VPN kommunizieren zu können. Dieser Ansatz wird im Übrigen auch von anderen Anbietern aufgegriffen, wenn auch nicht zur Behebung der NAT-Problematik: als Beispiel sei hier der so genannte Visitor Mode der Checkpoint VPN-1 genannt.

Schwerpunktthema

SCADA und IT-Security: Informations-Sicherheit in Automatisierungs- und Prozesskontrollsystemen

Dipl.-Phys. Stephan Beirer war während seines Studiums in Physik mehrere Jahre als freier Netzwerk-Administrator für verschiedene Institutionen und Unternehmen aus der LifeScience- und Medienbranche tätig. Zu seinen Schwerpunkten zählten dabei Lösungen zur Netzwerksicherheit sowie Konzeption und Betrieb von Server-Virtualisierungs-Lösungen, SAN-Netzen, IT-Sicherheit in Prozesskontroll- und Automatisierungs-Umgebungen, Remote-Access- und Firewall-Systemen. Herr Beirer ist seit 2006 als IT-Security Consultant bei der GAI NetConsult GmbH tätig. Er berät mittlere und große Unternehmen bei der Erstellung von organisatorischen und technischen Sicherheitsrichtlinien, bei der Implementierung eines IT-Sicherheitsmanagements nach ISO 27001 und bei der Notfallplanung.

Fortsetzung von Seite 1

Abbildung 1: Die moderne IT-Technologie wird auch in Automatisierungs- und Prozesskontrollumgebungen immer wichtiger

Diese Systeme sind häufig verteilt und dezentral aufgebaut, Steuergeräte wie zum Beispiel PLCs (Programmable Logic Controller, auf deutsch auch SPS: Speicherprogrammierbare Steuerung) überwachen und regeln autonom einzelne Prozessteile, während Telemetriedaten wie Druck- oder Geschwindigkeitsmesswerte über lokale Bussysteme an RTUs (Remote Terminal Units) und von dort dann an die Leitwarte übermittelt werden (siehe Abbildung 2). Hier werden die Daten weiter verarbeitet und die zentrale Prozesstechnik steuert und überwacht den Gesamtprozess und das Zusammenwirken aller Anlagen-Komponenten, indem sie bei Bedarf Steuerkommandos an die PLCs sendet. Im Leitstand werden die auflaufenden Daten auf so genannten Human-Machine-Interfaces (HMI) visualisiert und das momentane Abbild des Gesamtprozesses dargestellt. Das Bedienpersonal kann gegebenenfalls manuell in das System eingreifen und vom HMI aus Steuerbefehle an die PLCs senden. Zusätzlich verfügen SCADA-Systeme im Allgemeinen auch über weitere Backendsysteme, wie zum Beispiel Datenbanken (sog. Prozess-Historians), die das laufende Prozessabbild aufzeichnen und so eine spätere Auswertung der Daten ermöglichen. Eine DCS-Installation kann sich auf eine Produktionsanlage beschränken oder wie bei einem Pipelinesystem mit verschiedenen Pumpstationen, Ventilen und Drucksensoren räumlich sehr weit ausgedehnt und über mehrere Unternehmensstandorte verteilt sein, wobei die einzelnen Komponenten dann zum Beispiel über Richtfunkstrecken oder ähnliche Kommunikationssysteme verbunden sind. In besonders kritischen Installationen existieren meist mehrere Leitwarten an unterschiedlichen Standorten, die miteinander vernetzt sind und die redundant die Aufgaben eines ausgefallenen Systems übernehmen können.

Prozesssteuerungs- und Automatisierungs-Systeme kontrollieren häufig so genannte kritische Infrastrukturen (KRITIS), wie zum Beispiel Energie- und Trinkwasserversorgungsnetze, Öl- und Gasraffinerien oder Verkehrsleitsysteme. Aber auch abseits dieser kritischen Wirtschaftssektoren steuern sie in vielen Unternehmen die zentralen Produktions- und Versorgungsprozesse und zählen daher zu den sensiblen Geschäftsressourcen, die sich durch einen sehr hohen Schutzbedarf auszeichnen.

Während ursprünglich in der Prozesssteuerung und Anlagenüberwachung nur spezielle proprietäre Systeme und Individuallösungen verwendet wurden, veranlasste der steigende Kostendruck Hersteller und Anwender preisgünstigere Alternativen zu erwägen. In den letzen Jahren wurden deshalb herstellergebundene Kommunikationsprotokolle mehr und mehr durch einheitliche Normen ersetzt und Spezialkomponenten gegen Standardprodukte aus der IT-Technik ausgetauscht. Dadurch konnten Entwicklungs- und Anschaffungskosten gesenkt und die Interoperabilität zwischen den Systemen der verschiedenen Hersteller erhöht werden. Deshalb findet man in modernen Leitständen heute zum Beispiel Windowssysteme an den Operatorkonsolen, während auf den Backend-Rechnern gängige Enterprise-Da-

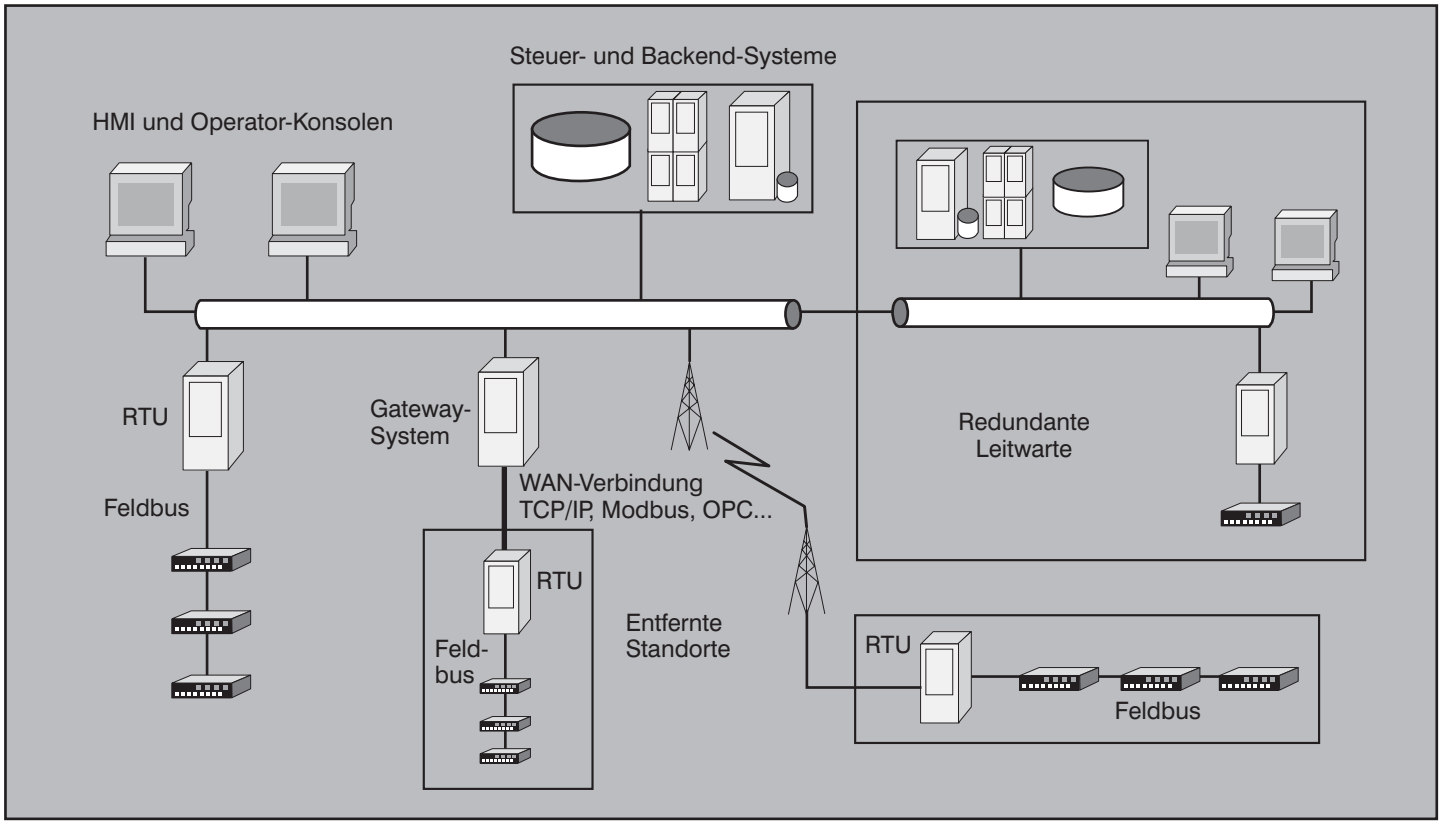


Abbildung 2: Schematische Darstellung eines DCS/SCADA-Systems

tenbanken unter Unix laufen. Parallel dazu werden die klassischen Feldbussysteme zunehmend gegen moderne Netzwerk-Technologien wie zum Beispiel Industrial Ethernet ausgetauscht und serielle Protokolle durch TCP/IP-basierte Standards ersetzt oder über IP-Netze getunnelt. Die Verwendung von einheitlichen Standards und Protokollen eröffnet dann auch neue Möglichkeiten zur umfassenden Datenintegration über Abteilungsgrenzen hinweg - so ist es zum Beispiel technisch viel einfacher das Ressourcen-Planungs-System im Enterprise-Netzwerk auf die Datenbank des Prozess-Historians zugreifen zu lassen, wenn in beiden Umgebungen TCP/IP und SQL verwendet wird.

Safety oder Security?

Die Einführung von Standard-Techniken aus der klassischen IT-Welt bringt allerdings auch neue technische und organisatorische Probleme mit sich, die bisher nur teilweise gelöst sind. Dies liegt unter anderem auch an den sehr unterschiedlichen Ansprüchen die in der Office-IT und in der Prozesssteuerung an die Technik gestellt werden müssen. Während zum Beispiel bei Büro-Fileservern variable Antwortzeiten in der Größenordnung von mehreren Sekunden tolerierbar sind, wird in Produktionsprozessen oft harte Echtzeitfähigkeit mit garantierten Antwortzeiten im Sub-Millisekundebereich gefordert.

Besonders offensichtlich treten die verschiedenen Anforderungen und die unterschiedliche technische Entwicklungsgeschichte der beiden Welten im Sicherheits-Bereich zu Tage. In der klassischen Unternehmens-IT ist mit dem Stichwort „Sicherheit“ normalerweise der englische Begriff der „Information Security“ gemeint - also der Schutz der Daten vor Verlust durch Hardwareschäden, vor unberechtigten Zugriffen oder böswilligen Angriffen. Im Prozessumfeld wird Sicherheit allerdings eher mit „Safety“ übersetzt, das heißt mit dem Schutz von Personen und Anlagen vor Schäden durch unbeabsichtigte Fehler und Geräteausfälle. Anhand des aus der Information Security bekannten CIA-Konzepts (Confidentiality, Integrity und Availability) lässt sich diese unterschiedliche Sicherheits-Auffassung etwas vereinfacht wie folgt darstellen: In der Enterprise-IT liegt die Betonung auf „Vertraulichkeit“ (Confidentiality), während in der Prozesstechnik mehr die „Verfügbarkeit“ (Availability) im Vordergrund steht. So werden im Office-Umfeld Daten durch restriktive Zugriffsrechte und Verschlüsselung vor Unbefugten geschützt, während im Prozessumfeld meistens von einem isolierten System mit zugangsberechtigtem Betriebspersonal als einzigen Systembenutzern ausgegangen wird. Umgekehrt ist in einem Prozessleitnetz jede relevante Betriebskomponente doppelt vorhanden (N-1 Redundanz), um die Anlagen-Verfügbarkeit jederzeit zu garantieren, während im Verwaltungsnetz oft nur die zentralen Systeme, wie zum Beispiel die Datenbank-Server ausfallsicher und hochverfügbar bereitgestellt werden. Diese unterschiedlichen Interpretationen des Sicherheits-Begriffs können oft zu Missverständnissen und Problemen beim Aufeinandertreffen von Prozesstechniker und IT-Administrator führen.

Neuartige Bedrohungen im Prozessumfeld

Aus der Sicht der Information Security birgt der Einsatz von Standard-IT-Komponenten in hochsensiblen Prozessnetzen und die heute oft anzutreffende direkte oder indirekte Kopplung des Prozess-LANs an das Office-Netzwerk ein stark unterschätztes Gefährdungspotential, das durch neuartige Sicherheitskonzepte kompensiert werden muss. Solch ein IT-Sicherheitskonzept für SCADA-Systeme muss für jedes Unternehmen individuell die verschiedenen potentiellen Bedrohungen abdecken - von gezielten Angriffen durch Cyber-Terroristen auf kritische Infrastrukturen bis hin zu unvorhergesehenen Seiteneffekten eines Softwareupdates durch den

IT-Administrator. Zu den neuartigen Bedrohungen für die Prozesstechnik zählen jetzt auch IT-basierte Angriffe von Innentätern, wie zum Beispiel der unzufriedene Angestellte, der das HMI-System mit einem aus dem Internet heruntergeladenen Exploit zum Absturz bringt. Oder der Einbruch eines Script-Kiddie-Hackers, der über einen Remote-Zugang in das Unternehmensnetz eingedrungen ist und mit einem DoS-Angriff unbewusst auch die ganze Leitwarte lahmlegt. Weitere Bedrohungen entstehen durch die schwächer werdende Isolation des Prozessnetzes vom Office-LAN, in einem Beispielszenario leitet dann der Router nach einer Fehlkonfiguration fälschlicherweise alle Broadcasts aus dem Office-Netz ins Prozess-LAN und verschlingt die für Echtzeitanwendungen nötige Bandbreite. Auch ohne direkte Netzkopplung ist eine vollständige Abschottung des Prozess-LANs heutzutage nur noch schwer zu realisieren: Ein Windows-Wurm kann auch durch den ungepatchten Laptop eines Wartungstechnikers eingeschleppt werden - er dringt dann zum Beispiel in die Operator-Konsolen ein, bringt diese zum Absturz und entzieht somit die gesamte Anlage der Kontrolle durch das Bedienpersonal. Auch die redundante Auslegung der Operator-Arbeitsplätze oder ganzer Leitwarten hilft hier nichts, wenn der Wurm selbständig alle erreichbaren Systeme befällt.

Alle die hier beispielhaft beschriebenen Szenarien sind in den letzen Jahren in produktiven Automatisierungs- und Prozesskontroll-Systemen Wirklichkeit geworden und haben dabei teils erhebliche Schäden verursacht, wie die folgende Auflistung zeigt:

- 1998 änderte ein verärgerter Angestellter eines großen Industrie-Unternehmens das Standard-Zugangspasswort eines PLCs im SCADA-System einer Nachbarabteilung, so dass daraufhin keine Wartung mehr möglich war. Um wieder Zugriff auf den PLC zu erhalten, musste das Bedienpersonal das Passwort des betroffenen Geräts zurücksetzen und dafür das gesamte Produktions-System für mehrere Stunden herunterfahren. [1]

- Während eines DCS-Systemupdates am Produktionsstandort einer Papierfabrik wurde technisches Personal aus der Firmenzentrale herangezogen, um die Installation unterstützend zu begleiten. Einer der beteiligten Ingenieure benötigt einige Wochen nach Abschluss der Arbeiten „frische“ Live-Daten, um seine Software besser testen zu können. Da er das Installationspasswort noch kannte und dieses inzwischen nicht geändert worden war, loggte er sich über eine Wartungsverbindung unbemerkt ins Prozessnetz der Papierfabrik ein. Auf dem Produktivsystem installierte er ein Programm, das alle 5 Minuten die Prozessdaten abfragte und sie ihm via Netzwerk in die Zentrale schickte. Unglücklicherweise überlastete dieser neue Job ein PLC-Gateway, so dass dieses über Monate immer wieder und in unregelmäßigen Abständen abstürzte und die Operatoren vor Ort so die Kontrolle über die von den PLCs gesteuerten Maschinen verloren. Die daraufhin veranlasste intensive Fehlersuche verursachte mehrere längere Produktionsausfälle und einen großen finanziellen Schaden. Da der verantwortliche Ingenieur inzwischen das Unternehmen verlassen hatte, wurde die wahre Ursache nur zufällig nach einer kompletten Überprüfung aller Systemkomponenten bemerkt [2].

- Ein Ausbruch des Nachi-Computerwurms im Netzwerk von CSX Transportation, einer der größten Eisenbahngesellschaften der US Ostküste, brachte im August 2003 zeitweise den gesamten Schienenverkehr im 37.000 km langen CSX-Netz zum Erliegen. Der Wurm, der eine DCOM-Sicherheitslücke auf Windowssystemen ausnutzte, beeinträchtigte die Kommunikation der elektronischen Dispatch- und Signalsysteme, so dass der Zugverkehr automatisch eingestellt wurde. Erst nach mehr als 5 Stunden konnten die ersten Strecken wieder in Betrieb genommen werden, die Wiederaufnahme des Normalbetriebs war erst nach 2 Tagen möglich.

- Bei DaimlerChrysler mussten im August 2005 an 13 Standorten die Fließbänder für mehr als eine Stunde angehalten werden, nachdem der Zotob-Wurm in die dortigen Prozesssteuerungsnetze eingedrungen war. 50.000 Angestellte konnten ihre Arbeit erst fortsetzen, nachdem die betroffenen Windows2000-Systeme gesäubert und gepatcht waren. Der finanzielle Schaden durch den Produktionsausfall wurde von einem Pressesprecher als „nicht unsignifikant“ bezeichnet. Zusätzlich befiel der Wurm auch einige der Zulieferfirmen des Automobilkonzerns, was die Produktion ebenfalls für mehrere Tage behinderte.

- Ein unbekannter Hacker drang im Oktober 2006 in den Laptop eines Wasserwerk-Angestellten und von dort über einen RAS-Wartungszugang in das Netzwerk eines städtischen Wasserversorgers ein. Auf den internen Systemen, die die Trinkwasseraufbereitung steuerten, installierte er Mailserver zum Spamversand und FTP-Server mit raubkopierter Software. Laut WaterISAC, einem Emergency Response Team der US-Trinkwasserversorger, kam es im Jahr zuvor auch zu einem gezielten DoS-Angriff auf die Systeme eines US-Wasserversorgungsunternehmens [3].

- Im Jahr 2000 wurde bekannt, dass es Hackern gelungen war, in die Pipeline-

Kontrollsysteme des weltgrößten Erdgaslieferanten Gazprom einzudringen. Laut offiziellen Angaben war das zentrale Gas-Verteilsystem „für einige Zeit“ unter der Kontrolle der Angreifer.

Auf Grund des zu befürchtenden Reputationsverlusts werden vermutlich viele ähnlich geartete Vorfälle von den betroffenen Unternehmen gar nicht erst veröffentlicht. Das auf SCADA-Sicherheit spezialisierte Internet Engineering Lab des British Columbia Institutes of Technology (BCIT/IEL) betreibt eine vertrauliche und anonymisierte Datenbank zur Sammlung von IT-Sicherheits-Incidents in Prozessnetzen [4]. Die Datenbank enthält Informationen zu über 120 Vorfällen (Stand: Ende 2005), von denen die meisten nicht öffentlich bekannt wurden. Interessanterweise zeigt eine Analyse der Daten, dass im Zeitraum von 1982 bis 2000 69 Prozent der Vorfälle von Innentätern verursacht wurden oder auf Fehler von Angestellten zurückzuführen waren, während 31 % externen Angreifern zuzuschreiben waren. Seit 2001 hat sich diese Statistik stark gewandelt: Inzwischen sind 70% der seitdem gemeldeten 57 Sicherheitsvorfälle als Angriffe von externen Tätern klassifiziert. Auch wenn eine statistische Auswertung solcher Daten grundsätzlich schwierig sein wird, ist hier ein eindeutiger Trend zu erkennen, der sicher auch darauf zurückzuführen ist, dass eine konsequente Isolierung der Prozessnetze heutzutage kaum noch anzutreffen ist, auch wenn das von vielen Verantwortlichen häufig noch behauptet wird [5]. Beängstigend ist auch, dass seit 2002 20 % der Vorfälle als gezielt gegen SCADA-Systeme gerichtete Angriffe identifiziert wurden.

Zahlreiche Problemfelder

Eine Analyse der oben aufgelisteten Bedrohungsszenarien und der bekannt gewordenen Sicherheitsvorfälle zeigt, dass sich in den heutigen heterogenen Prozessnetz-Umgebungen folgende allgemeinen Problembereiche der IT-Sicherheit identifizieren lassen:

Prozesssteuerungssysteme sind Anlagenbestandteile

Diese auf den ersten Blick triviale Aussage hat weit reichende Konsequenzen: die IT-Systeme zur Steuerung der entsprechenden Prozessanlagen werden vom Anlagenhersteller mitgeliefert - und entziehen sich meist den im Unternehmen geltenden Standards für IT-Systeme (unterstützte Betriebssysteme, Verzeichnisdienste, System- und Managementumgebungen etc.). Oftmals werden sie auch komplett von den zuständigen Fachabteilungen und nicht von der zentralen IT betrieben. Diese Fachabteilungen haben ihren Know-how Schwerpunkt aber eher im Bereich der eigentlichen Prozessabläufe bzw. der Prozesssteuerung - und nicht auf dem Gebiet der IT-Sicherheit. Dies betrifft oft auch die mit einer Anlage gelieferten Bedienarbeitsplätze und Technikernotebooks, die dann ohne Einbindung in die zentralen IT-Prozesse (wie zum Beispiel Patch- und Updatemanagement, Virenschutzaktualisierung) betrieben werden. Bei individuellen Applikations- und Systementwicklungen durch einen externen Dienstleister wird außerdem der Bereich der IT-Sicherheit im Pflichtenheft meist ausgespart.

Anlagen haben andere Zeithorizonte

Industrieanlagen sind für ganz andere Nutzungszeiten vorgesehen, als dies im IT-Bereich üblich ist. Die Infrastruktur einer Ölraffinerie kann nicht im 5-Jahrestakt erneuert werden. Wegen der derzeit noch üblichen engen Verknüpfung zwischen Anlage und Prozesssteuerung gilt dies dann auch für die IT-Systeme - auch wenn es sich hierbei mittlerweile zumeist um handelsübliche Standardrechner und Betriebssysteme wie Solaris oder Windows handelt. Somit sind auch heutzutage noch viele Systeme in Benutzung, die vor mehr als 10 Jahren geplant bzw. installiert worden sind. Inzwischen haben sich die Umgebungen, für die die Systeme entworfen wurden, aus Sicherheitssicht aber grundlegend geändert: Während damals oft vom ideal isolierten System ausgegangen wurde, in dem es nur vertrauenswürdige Nutzer gibt, ist es heute leicht möglich, dass durch die zunehmende direkte oder indirekte Kopplung mit anderen Netzwerken auch externe Nutzer Zugang zum Prozessnetz haben beziehungsweise leicht erlangen können. Die Zugangs- und Zugriffschutzmechanismen, die in den heutigen Einsatzumgebungen nötig wären sind in den Systemen nicht vorhanden und können meist auch nicht einfach nachgerüstet werden. Die Entwicklung solcher Anlagensysteme ist außerdem sehr komplex und folgt deshalb grundsätzlich anderen Zeithorizonten, so liefern viele Hersteller auch noch heute Neuanlagen mit (aus IT-Sicht) völlig veralteten Rechnersystemen aus, zum Beispiel ist Windows NT mit SP1 im Prozessumfeld noch oft anzutreffen. Es ist offensichtlich, dass solche Systeme anfällig gegen eine Vielzahl von lange bekannten Angriffen sind. Hinzu kommt häufig auch ein wirtschaftlicher Aspekt: die Geldmittel für eine Erneuerung der Prozesssteuersysteme innerhalb der Betriebsdauer der Gesamtanlage wurden schlicht nicht eingeplant, da eine derartige Entwicklung der IT-Technologie durch die Anlagenbetreiber nicht vorhergesehen wurde.

Fehlendes Patch- und Updatemanagement

Unter anderem aus den beiden vorgenannten Gründen sind viele Prozesssysteme nicht in ein zeitnahes Patch- und Updatemanagement eingebunden. Dies ist oftmals aber auch gar nicht so einfach möglich, da bei vielen Anlagen Änderungen an den Steuersystemen nicht im laufenden Betrieb zulässig sind und eine Abschaltung teuer und aufwändig wäre. Gleiches gilt für räumlich weit verteilte Anlagen wie zum Beispiel Gas- und Stromnetze, bei denen gegebenenfalls die Techniker für Updates vor Ort erscheinen müssten. Hinzu kommt, dass aufgrund des Alters der Rechner und Betriebssysteme ein Update auf einen aktuellen, sicheren Stand schlicht und ergreifend nicht mehr möglich ist. Ein weiteres Problem ist, dass die bestehenden gesetzlichen oder unternehmensinternen Vorschriften und Regularien oft eine weitgehende Neuabnahme der Anlage bei derartigen Änderungen an den Prozesssteuersystemen vorsehen. Manchmal geht dies soweit, dass die Aktualisierung der Virenpattern einen 14-tägigen Prüfprozess nach sich zieht, was die Häufigkeit der Updates verständlicherweise stark begrenzt. Die Konsequenzen liegen dann auf der Hand: die Systeme bleiben im Auslieferungszustand und haben vielfältige Sicherheitslücken, die von Angreifern mit Zugang zum Prozessnetz, aber auch von Würmern, die - wie auch immer - in diesen Netzbereich hineingelangten, ausgenutzt werden können. Auch wenn darüber dann noch kein direkter Eingriff in die Prozesssteuerung möglich ist, kann doch die Verfügbarkeit massiv eingeschränkt werden. Dies hat bei den meisten Prozessanlagen über kurz oder lang zur Folge, dass die Anlage in einen instabilen Zustand gerät und abgeschaltet werden muss oder dies vorsorglich gleich selbst tut - und genau das ist in Prozessumgebungen oft bereits der Worst Case.

Unsichere Protokolle ohne Authentisierung

Die einzelnen Komponenten einer Industriesteuerung tauschen in der Regel untereinander selbständig Nachrichten und Steuerkommandos aus, ohne dass eine Authentisierung des jeweiligen Partners erfolgt. Das gilt oft auch für die manuellen Steuerbefehle, die von den Leitrechnern aus abgegeben werden. Dieses Problem ist grundsätzlicher Natur, denn alle relevanten Industrie-Kommunikationsstandards wie zum Beispiel Modbus oder die IEC-Protokolle sehen eine Authentisierung oder Verschlüsselung überhaupt nicht vor. Außerdem verfügen diese Protokolle über keine oder aber sehr einfach zu erratende

Sequenznummern oder Timestamps. Damit ist für einen Eindringling im Prozess-LAN ein Replay-Angriff, bei dem bereits gesendete Pakete nochmals eingespielt werden, sehr leicht durchführbar. Aufgrund der in industriellen Installationen oft anzutreffenden Embedded Systeme ist es technisch auch gar nicht möglich Authentisierung oder gar Verschlüsselung in die Protokolle zu integrieren, da die verwendeten Prozessoren gar nicht über genügend Rechenleistung verfügen.

Keine vollständige Trennung der Netze

Es ist offensichtlich, dass die Sicherheit derartiger Prozesssteuerungen nur bei konsequenter Isolierung der Prozessnetze gewährleistet werden kann. Hier sehen wir aber in drei Bereichen immer wieder, dass diese Abschottung mehr und mehr aufgeweicht wird: Die Zahl externer Wartungszugänge nimmt unter anderem wegen des Kostendrucks auch im Produktionsumfeld stark zu. Aufgrund der Bandbreitenanforderungen werden dabei auch Standleitungen zu externen Lieferanten, zum Teil ohne personengebundene Authentisierung genutzt. Auch innerhalb der Unternehmen werden immer häufiger Forderungen laut, von jedem Standort und auch von mobilen Systemen aus auf die Produktions- und Prozessumgebungen zugreifen zu können. Immer stärker integrierte Prozesse erfordern auch eine Übermittlung von Prozessdaten in andere IT-Bereiche. Auch wenn viele Unternehmen die Kopplungen über Security-Gateways und gegebenenfalls zwischengeschaltete Proxy-ähnliche Systeme vornehmen, erhöhen sich hierdurch die Risken durch einen unberechtigten Zugriff auf die Produktionsbereiche. Gerade in Hinblick auf die Anfälligkeit gegen Wurmattacken ist es unseres Erachtens besonders problematisch, dass Notebooks eigener und fremder Servicetechniker an die Prozessnetze angeschlossen werden, die auch für andere Zwecke - bis hin zum normalen Internetzugriff - genutzt werden.

Unsichere Basistechnologien und Default-Einstellungen

Die in der Prozesstechnik eingesetzten Anwendungen und Protokolle bauen inzwischen häufig auf Systemen und Technologien auf, die ursprünglich nicht für hochverfügbare oder sensible Umgebungen konzipiert wurden. So basiert zum Beispiel das im Prozessumfeld häufig anzutreffende Protokoll OPC (Openness, Productivity, Collaboration, vormals: OLE for Process Control) auf DCOM, welches auf eine lange Geschichte von Sicherheitsproblemen zurückblicken kann. Beispielsweise nutzen einige der Windows-Würmer, die in den letzten Jahren für Aufsehen gesorgt haben, DCOM-Sicherheitslücken aus. Auch wenn diese Sicherheitslücken nicht direkt das OPC-Protokoll betreffen, kann ein Wurmbefall zum Beispiel den DCOM-Dienst zum Absturz bringen oder durch den massiven Wurm-Verkehr auf dem DCOM-Port die Prozesskommunikation stark beeinträchtigen. So war zum Beispiel ein Windows-Wurm die Ursache für den Ausfall eines sekundären KKW-Kontrollsystems in den USA und auf Grund der bekanntgewordenen Fakten ist es auch zu vermuten, dass die Beeinträchtigung der OPC-Kommunikation der Grund für den oben beschriebenen Zusammenbruch des CSX-Eisenbahnnetzes war. Auch wenn DCOM die Möglichkeit zu granularen Zugriffsbeschränkungen und verschiedene Sicherheitseinstellungen bietet, stellen wir meist fest, dass der Remote-Zugriff dann doch für die Gruppe ‚Everyone' freigegeben wird – aus Bequemlichkeit oder um widerspenstige Systeme zur Zusammenarbeit zu bringen. Die vom Hersteller gesetzten Default-einstellungen sind deshalb auch meist für eine einfache Installation und auf maximale Interoperabilität optimiert, anstatt hier werksseitig für ein angemessenes Basis-Sicherheitsniveau zu sorgen.

Angriffe erfordern wenig spezielles Know-how

Betreiber von Prozesssteuerungen betonen oft, dass für die Bedienung der Anlagen sehr spezielles Fachwissen erforderlich sei. Das mag sein, unsere Erfahrung zeigt aber, dass Angriffe gegen die Prozesssysteme meist schon auf dem Niveau von Betriebssystem und Basiskomponenten wie zum Beispiel X11 möglich sind. Wenn ein Angreifer über eine beliebige Schwachstelle in das Betriebssystem der Leitwartenrechner eindringen konnte, ist es in der Regel dann auch kein Problem, Zugriff auf die graphische Bedienoberfläche der Leitstand-Applikation zu erhalten und von dort beliebige Befehle auszulösen. Dies erlaubt dann oftmals schon die Einschränkung der Anlagen-Verfügbarkeit. Deshalb ist es meist gar nicht erforderlich, in die sehr spezielle Low-Level-Prozesskommunikation einzugreifen, um die Systeme erfolgreich anzugreifen. Aber auch auf der Ebene der Prozessprotokolle bieten sich Angriffsmöglichkeiten, die kein vertieftes Prozess-Know-how oder Insider-Kenntnisse erfordern und trotzdem schon massive Auswirkungen auf die Anlagen haben, zum Beispiel durch das massenhafte Erzeugen von zufälligen oder fehlerhaften Datenpaketen (Protokoll-Fuzzing). In unseren Testaufbauten war es auch möglich nach einfachen Protokollanalysen durch Replay-Attacken PLC-Ausgänge anzusteuern oder die Geräte gezielt abzuschalten.

Lösungsansätze

Die hier geschilderten grundsätzlichen Problemfelder zeigen deutlich, dass zum Erreichen eines angemessenen Sicherheitsniveaus in Prozesskontrollumgebungen nicht einfach die bewährten Sicherheitsmassnahmen aus der Enterprise-IT übernommen werden können. Es ist auch offensichtlich, dass punktuelle Einzelmaß-

nahmen, wie die Installation einer Security-Appliance oder Firewall, nicht ausreichend sind. Aufgrund der Verschiedenheit der Anlagen existieren für SCADA-Systeme bisher auch kaum Best-Practice-Ansätze für typische Installations-Szenarien. Deshalb ist für jede Anlage immer eine individuelle Risiko-Analyse notwendig, um das vorhandene Gefährdungspotential zu erkennen und durch entsprechende Gegenmaßnahmen in einem Sicherheitskonzept zu minimieren. Zusätzlich zeichnen sich die betrachteten Systeme generell auch durch eine starke Heterogenität und große Komplexität bei einem gleichzeitig sehr hohen Schutzbedarf aus. Aus diesen Gründen ist im Allgemeinen ein umfassender und systematischer Sicherheits-Prozess notwendig, der organisatorisch als Information Security Management System (ISMS) im Unternehmen implementiert werden sollte. Solch ein Sicherheits-Prozess für SCADA- und Automatisierungssysteme kann in ein schon bestehendes, unternehmensweites Information Security Management System integriert werden, es kann aber auch ein eigenständiges ISMS aufgebaut werden, dessen Geltungsbereich auf die Prozesstechnik-IT beschränkt ist. Dabei sollten die in der Enterprise-IT etablierten Standards wie ISO 27001/17799 als Leitlinien dienen. Der ISO17799-Ansatz ist hier auch besonders vorteilhaft, weil er nicht spezifisch auf eine Office IT-Umgebung ausgerichtet ist und deshalb auch nicht erst umständlich an das SCADA-Umfeld angepasst werden muss. So sind zum Beispiel keine größeren Änderungen an den in ISO17799 definierten Standard-Kontrollzielen oder zusätzlichen Kontrollziele für die Prozessumgebungen nötig. Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene IT-Grundschutz-Standard ist hier unflexibler, da er von vorneherein gewisse Annahmen über die in der betrachteten IT-Umgebung eingesetzte Technik und deren Schutzbedarf macht. Die im Rahmen des ISMS zu definierenden Security-Richtlinien und die spezifischen Sicherheitsmassnahmen müssen natürlich an die besonderen technischen Ansprüche von Prozessumgebungen angepasst werden, wobei dann auch die unternehmensspezifischen Anforderungen berücksichtigt werden müssen. Hier hat das BSI Mitte 2005 eine Beispiel-Sicherheitsrichtlinie für KRITIS-Unternehmen veröffentlicht, die auch einen kurzen Abschnitt über Prozesskontrollsysteme enthält [6]. Dieses Dokument kann als Grundlage bei der Erstellung einer eigenen Security-Richtlinie und bei der Wahl geeigneter Sicherheitsmaßnahmen dienen.

Beim Aufbau des ISMS und bei der Implementierung und kontinuierlichen Anwendung der Sicherheitsmassnahmen ist besonders darauf zu achten, dass sowohl das technische Know-how der anlagenbetreibenden Fachabteilung als auch IT-spezifisches Fachwissen integriert werden. Ansonsten besteht die Gefahr, dass der Sicherheitsprozess essentielle betriebstechnische Anforderungen nicht berücksichtigt oder wichtige IT-Sicherheitsaspekte ignoriert werden und die Sicherheitsmassnahmen dann gar nicht beziehungsweise nicht ausreichend effektiv umgesetzt werden können. Gegebenenfalls muss das ISMS deshalb abteilungsübergreifend und unternehmensweit aufgebaut werden.

Die Entwicklung und Umsetzung eines SCADA-Sicherheitskonzepts und die Etablierung eines entsprechenden ISMS-Prozesses ist ein arbeitsintensives Projekt, das nicht unterschätzt werden sollte. Insbesondere in der Planungsphase und in der Anlaufzeit kann die Unterstützung durch einen kompetenten Dienstleister sehr hilfreich sein.

Richtlinienbeispiele für SCADA-Systeme

Da die Implementierung eines ISMS für Prozesstechnikumgebungen, die aufzustellenden Security-Richtlinien und die umzusetzenden Sicherheitsmassnahmen je nach Unternehmen und zu schützender Anlage sehr verschieden sein können, wollen wir im Folgenden nur beispielhaft einige der SCADA-spezifischen Punkte auflisten, die in Abhängigkeit von der Struktur des vorliegenden Prozesskontroll-Systems berücksichtigt werden sollten.

- Die Kommunikationsinfrastruktur ist ein integraler und hochsensibler Bestandteil eines Kontrollsystems und muss besonders geschützt werden. Für den Aufbau des SCADA-Netzes müssen deshalb eigene, dezidierte Netzwerkkomponenten verwendet werden. Bei besonders hohem Schutzbedarf ist auch von der Verwendung von VLANs innerhalb der Prozessnetze abzusehen, stattdessen sollten ebenfalls eigenständige Komponenten verwendet werden. Falls der Einsatz von gemeinsam genutzten Hardware-Ressourcen nicht vermieden werden kann, zum Beispiel bei WAN-Kopplungen oder RAS-Zugängen, ist hier besonders der Verfügbarkeitsaspekt zu berücksichtigen.

- Das BSI empfiehlt in seiner KRITIS-Beispielrichtlinie das Netzwerk eines Prozesskontroll-Systems in nach Funktion und Schutzbedarf getrennte Schichten aufzuteilen und die Kopplung mit externen Netzen über eine DMZ (Demilitarized Zone) zu realisieren (siehe Abb. 3)

  1. DCN: Das DCN (Distributed Control Network) umfasst Sensoren und Steuergeräte zur Überwachung und Regelung der Anlagen. Der interne Aufbau des DCN ist meistens herstellerspezifisch und verwendet unter Umständen eigene Protokolle.

  2. PCN: Im PCN (Process Control Network) befinden sich die geschäftskritischen Systeme, die direkt mit den Anlagensteuerungen interagieren. Deshalb ist der Zugriff auf diese PCN-Systeme stark einzuschränken und gut abzusichern.

  3. PIN: Im PIN (Process Information Network), das als DMZ ausgelegt ist, befinden sich die Systeme, die sowohl von den PCN- als auch von externen Büronetzwerk-Systemen genutzt werden. Im PIN wird ein Mechanismus für einen sicheren Datenaustausch zwischen den beiden Netzwerken bereitgestellt, ohne eine direkte Verbindung zwischen ihnen herzustellen.

- Das Securitygateway-System beschränkt und regelt die Kommunikation zwischen den einzelnen Netzwerkzonen. Je nach Bedarf kann es aus einer Kombination von Firewall, Antiviren- und Content-Scannern sowie IDS/IPS-Systemen bestehen. Eine direkte Kommunikation zwischen PCN und Büronetz findet nicht statt, ein Datenaustausch sollte möglichst über Offline-Medien wie zum Beispiel CD-ROMs erfolgen, die auf vom SCADA-Netz isolierten Systemen auf Viren oder ähnliche Malware geprüft werden. Wenn eine Echtzeitkommunikation stattfinden muss, wird die Verbindung durch einen in der PIN-DMZ aufgestellten und speziell gehärteten Applikationsproxy vermittelt, der möglichst auch eine Content-Überprüfung auf Viren und ähnliche Schadsoftware vornimmt. Vom Büronetz ist der Zugriff auf die Systeme in der PIN-DMZ auf explizit berechtigte Benutzer und Systeme beschränkt, falls möglich sollte der Verbindungsaufbau auch immer aus der DMZ ins Büronetz hinein erfolgen, damit Verbindungen in umgekehrter Richtung an der Firewall generell geblockt werden können.

- Besonders bei räumlich verteilten Installationen mit vielen Gerätestandorten sollte das Netzwerk auch horizontal in Standort-Segmente aufgeteilt werden. Diese werden über Router oder

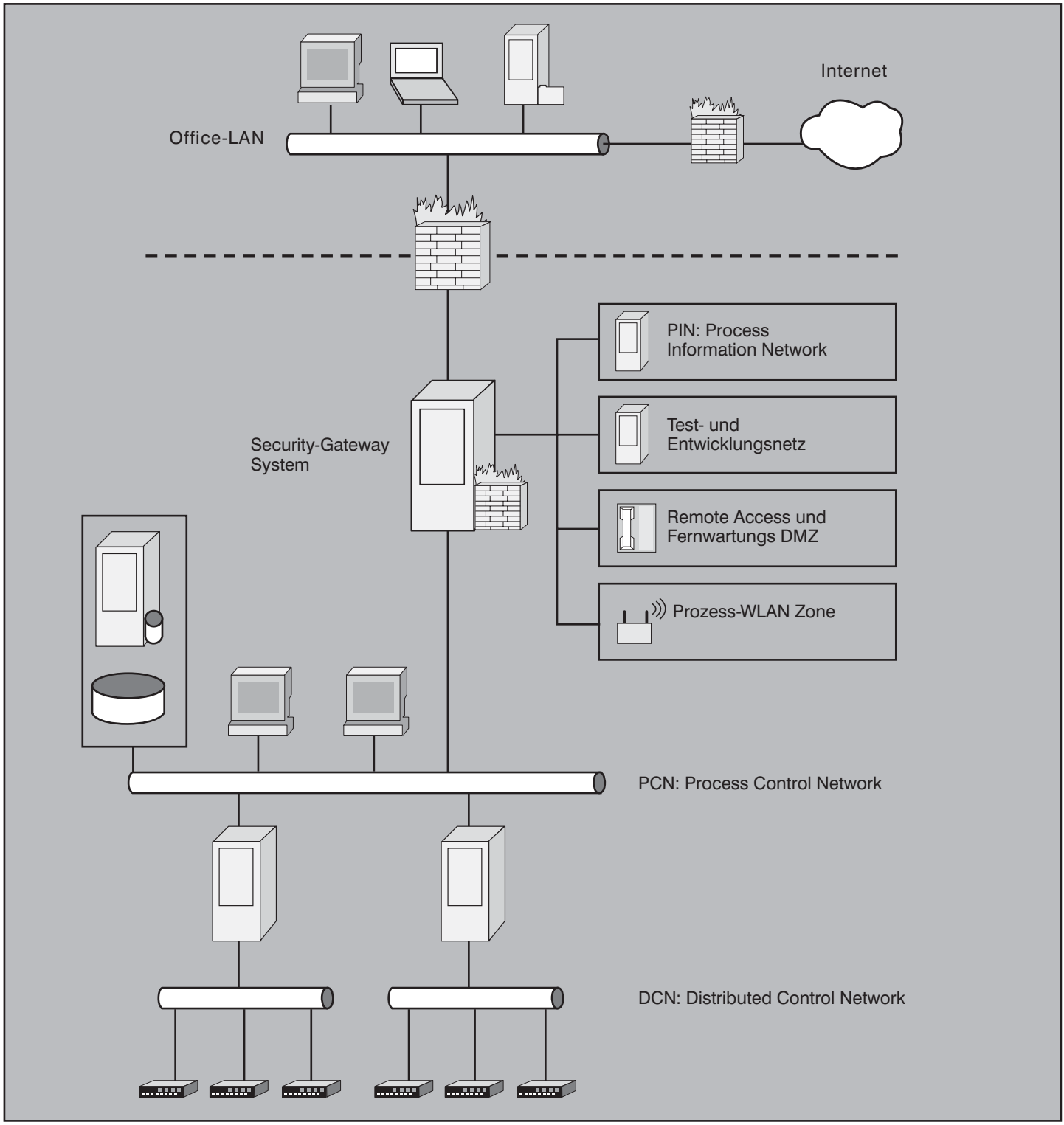


Abbildung 3: Überblick zur empfohlenen Netzwerkarchitektur für Prozesskontrollsysteme

falls möglich über Firewalls an das übrige Netz gekoppelt. Beim Einsatz von Firewalls wird die Kommunikation zwischen den einzelnen Segmenten und Geräten auf das erforderliche Minimum eingeschränkt. Dies gilt besonders dann, wenn die physikalische Sicherheit der einzelnen Standorte nur schwer sicherzustellen ist, zum Beispiel bei unbemannten Pumpstationen. So wird verhindert, dass ein Angreifer, der Zugang zu einem der Systeme erlangt hat, über die Netzwerkverbindung ungehindert auf alle anderen Komponenten zugreifen und diese kompromittieren kann. Müssen Daten zwischen den Segmenten über Router- und Firewall-„unfreundliche“ Protokolle wie OPC ausgetauscht werden, sollten diese beispielsweise mit einem TCP-Protokolltunnel übertragen werden (siehe z.B.

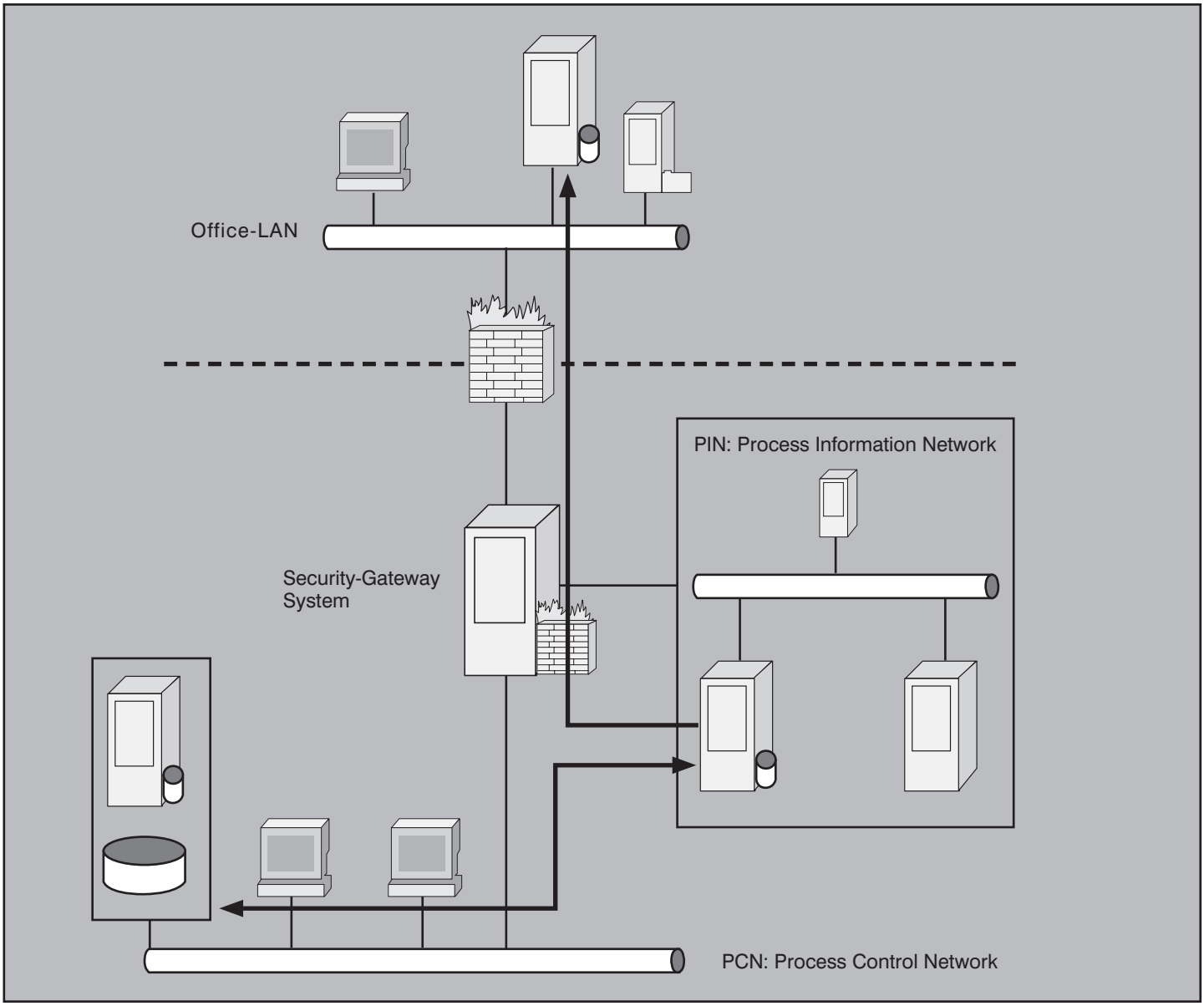


Abbildung 4: Datenaustausch zwischen Prozessnetz und Office-LAN darf nur über die PIN-DMZ erfolgen

[7]), so dass auf der Firewall dann nur der Tunnel-Port freigeschaltet werden muss.

- Für die Verbindung mehrerer Prozessnetze, zum Beispiel an verschiedenen Standorten werden direkte Telekommunikationsverbindungen, beispielsweise Mietleitungen verwendet. Funkverbindungen sollten nur nach einer ausführlichen Risikoanalyse eingesetzt werden. Nur wenn die Verfügbarkeit und Ausfallsicherheit der Verbindung zwischen den Netzen für den Anlagen-Betrieb unkritisch ist, kann der Prozessnetz-Verkehr mittels authentisierter und verschlüsselter VPN-Verbindungen auch über die vorhandenen Büronetzwerkverbindungen geleitet werden. Eine Kopplung über öffentliche Internetverbindungen darf nie erfolgen.

- Daten, die in Systeme und Anwendungen im Prozessnetz importiert werden sollen (zum Beispiel Office-Dokumente oder Software-Updates), müssen grundsätzlich auf einem vom Prozessnetz isolierten Rechner auf Schadsoftware geprüft werden, bevor sie ins System eingespielt werden.

- Entwicklungs- und Testsysteme dürfen nicht in produktiven Netzen betrieben werden, sondern müssen ebenfalls in einem eigenen Test-Segment installiert werden, das durch ein Security-Gateway von den übrigen Netzen getrennt ist. Wenn es unvermeidbar ist, dass die Testsysteme Zugriff auf einzelne Komponenten im Produktivnetz, zum Beispiel auf Sensoren oder Steuergeräte benötigen, darf dieser nur selektiv freigegeben werden und muss nach Wegfall der Anforderungen wieder entfernt werden. Wann immer möglich sollten Software-Updates zuerst in komplett isolierten Entwicklungs-Systemen getestet werden.

- Alle Netze, die nicht unter der Kontrolle des Prozesssteuerungs-Personals stehen, wie zum Beispiel die Netze externer Dienstleister oder die Wartungszugänge der Anlagen-Hersteller und Außendienst-Mitarbeiter sind als nicht vertrauenswürdig einzustufen. Solche Zugänge dürfen nicht direkt mit dem

PCN verbunden werden, sondern müssen ebenfalls in einer eigenen RAS-DMZ terminiert werden. Zusätzlich sind sie durch starke 2-Faktor-Authentifizierung zu sichern und gegebenenfalls nur nach Autorisierung durch das Bedienpersonal freizuschalten. Aus der RAS-DMZ heraus können dann zum Beispiel Terminalserver den Zugang zu den benötigten Systemen oder Applikationen vermitteln. Alle RAS-Zugänge werden einem periodischen Sicherheits- und Penetrations-Test unterzogen. Der Zugang externer Dienstleister zur DMZ ist auch bei der Fremdfirma vor Ort auf möglichst wenige Systeme zu beschränken, wobei diese ebenfalls auf einem hohen Schutzniveau abzusichern sind. Dies ist mit dem Dienstleister vertraglich zu vereinbaren und gegebenenfalls durch einen externen Auditor zu überprüfen.

- Wenn zu Wartungszwecken Notebooks an das Prozessnetz angeschlossen werden müssen, zum Beispiel bei verteilten Systemen in den einzelnen Standorten vor Ort, müssen diese speziell gehärtet sein und über aktuelle Sicherheitspatches und AV-Software verfügen. Diese Wartungsnotebooks dürfen auch sonst nur in vertrauenswürdigen Netzen mit hohem Schutzniveau benutzt werden und zum Beispiel nicht direkt mit dem Internet verbunden werden. Für externe Firmen wie Dienstleister oder Anlagenhersteller ist der Anschluss von eigener Hardware an das Prozessnetz nur in Ausnahmen zulässig, dann sind die oben genannten Maßnahmen ebenfalls vertraglich zu vereinbaren.

- Bei sehr hohem Schutzbedarf oder wenn das Patchen verwundbarer Systeme aus oben genannten Gründen nicht möglich ist, können in den einzelnen Netzsegmenten Intrusion Detection und Prevention Systeme (IDS/IPS) installiert werden, die Angriffe oder das Eindringen von Würmern und Viren frühzeitig erkennen und blockieren können. Da diese Systeme aber sehr betreuungsintensiv sind und tiefgehendes Security-Fachwissen erfordern, sollte die Überwachung des IDS an einen Sicherheits-Serviceprovider ausgelagert werden (Security Event Monitoring). Inzwischen gibt es am Markt auch IDS-Systeme, die einige der verbreiteten SCADA-Protokolle verstehen und dafür auch Events generieren können. Vom Einsatz von SCADA Intrusion Prevention Systemen (IPS) raten wir in produktiven Umgebungen allerdings ab, da ein Fehlalarm hier gegebenenfalls eine gewollte, kritische Aktion blockieren könnte.

- Es sollten Vorkehrungen getroffen und ein entsprechender Krisenplan aufgestellt werden, anhand dessen bei einem akuten kritischen Sicherheitsvorfall innerhalb des Büronetzes das Prozessnetz komplett isoliert werden kann. Dabei ist zu beachten, dass dann eventuell wichtige Applikationen nicht mehr über die Netzgrenzen kommunizieren können. Das Feststellen eines solchen kritischen Zustands darf auch nur anhand definierter Vorgaben und nach Rücksprache der Sicherheitsverantwortlichen in den betroffenen Netzen geschehen. Sollte eine vollständige Trennung nicht durchführbar sein, muss der Plan die maximal möglichen Kommunikations-Beschränkungen spezifizieren, die bei Bedarf in Kraft gesetzt werden können. Ein Verfahren zum Wiederanbinden der beiden Netze muss ebenso festgelegt werden.

- Die IT-Systeme in der Prozesskontroll-Umgebung werden wenn möglich gehärtet und durch Antivirensoftware geschützt, in ein Updatemanagement aufgenommen und zeitnah gepatcht. Hierbei ist aber unbedingt zu beachten, dass anderslautende Herstellerhinweise zu Systemhärtung und zur Installation von AV-Software und Sicherheitsupdates gegenüber den unternehmensinternen Regelungen Vorrang haben müssen. Den Herstellerhinweisen widersprechende Empfehlungen werden nur nach gründlichen Tests implementiert.

- Bei Neubeschaffungen und Neuentwicklungen von Komponenten und Applikationen muss die IT-Sicherheit explizit berücksichtigt, vom Hersteller gefordert und in den Anforderungen auch detailliert beschrieben werden. Die Systeme sollten zum Beispiel die oben genannte System-Härtung und das Einspielen von Sicherheitsupdates auf einfache Art und Weise erlauben. Vor Inbetriebnahme wird die Erfüllung der IT-Sicherheitsanforderungen überprüft und dokumentiert, bei kritischen Komponenten werden diese auch einem Penetrations- und Stresstest unterzogen. In den Wartungsverträgen muss auch die Bereitstellung von sicherheitsrelevanten Systemupdates durch den Hersteller gefordert werden.

- Die Verwendung von WLAN-Technologien sollte in Prozesskontroll-Umgebungen soweit wie möglich ausgeschlossen werden. Gibt es zum WLAN-Einsatz keine vernünftigen Alternativen, wird das Funknetz in einem eigenen Netzsegment betrieben, das durch eine restriktiv eingestellte Firewall abgetrennt ist. Das WLAN ist nach dem Stand der Technik sicher zu konfigurieren, wobei der der aus Sicherheitssicht schwache WEP-Verschlüsselungsstandard zu vermeiden ist.

- Die Überprüfung von produktiven SCADA-Systemen auf vorhandene Sicher-

heitslücken durch aktive Scans und sogenannte „Penetrationstests“ ist in Sicherheitskreisen sehr umstritten und wird von den Verantwortlichen meistens nicht zugelassen. Unsere Erfahrung zeigt, dass solche Systeme auch unter „non-intrusive“ und als sicher geltende Tests wie zum Beispiel simplen Portscans häufig abstürzen oder in undefinierte Zustände übergehen, was im Produktiv-System trotz vorhandenen Redundanzkomponenten kritische Auswirkungen haben kann. Deswegen sollten solche Überprüfungen vorzugsweise in isolierten Testumgebungen stattfinden. Generell gilt aber, dass die Systeme so robust entwickelt werden müssen, dass sie Standardtests ohne Probleme überstehen; dieser Punkt muss bei Neuanschaffungen berücksichtigt, gefordert und auch überprüft werden.

- Die Datensicherung sollte nicht über Netzgrenzen hinweg, sondern lokal im Prozessnetz auf dezidierten Backup-Systemen erfolgen. Ein Sicherungssatz wird dabei außerhalb des Standortes hinterlegt. Für die System-Wiederherstellung müssen dokumentierte und getestete Recovery-Prozeduren und Wiederanlaufpläne existieren.

Fazit

Die vorangegangene Betrachtung hat deutlich gezeigt, dass die Einführung von Systemen und Technologien aus der klassischen IT-Welt in Automatisierungs- und Prozesskontrollumgebungen neben den offensichtlichen Vorteilen wie Kostenreduktion und erhöhter Flexibilität auch neuartige und schwerwiegende Sicherheitsrisiken mit sich gebracht hat. Um diese Risiken zu minimieren und kontrollieren zu können sind neue und angepasste IT-Sicherheitsansätze notwendig, da die bisherigen Information-Security-Konzepte aus der Enterprise-IT nicht einfach auf Prozesskontrollumgebungen übertragen werden können. Um den speziellen Anforderungen von Prozesssteuerungs- und Automatisierungs-Systemen gerecht zu werden und dem meist sehr hohen Schutzbedarf von Produktionsanlagen und Verteilnetzen zu genügen, muss im Unternehmen ein individueller und auf SCADA-Systeme angepasster ISMS-Prozess etabliert werden. Durch geeignete, an die Anforderungen der jeweiligen Anlage angepasste IT-Sicherheitsmaßnahmen muss ein ausreichendes Sicherheitsniveau erreicht werden, dass die volle Verfügbarkeit und Funktion der Anlage jederzeit sicherstellt und gleichzeitig ihren Betrieb nicht behindert. So muss beispielsweise die Architektur der Prozessnetze dem hohen Schutzbedarf angepasst werden, um das System so gut wie möglich zu isolieren und sicherzustellen, dass der Datenaustausch mit anderen Netzen wie dem Büronetz oder über Wartungszugänge nur auf sichere und kontrollierte Weise erfolgen kann. Es ist klar, dass die Einführung eines solchen ISMS und die Ausarbeitung geeigneter Sicherheitskonzepte und -maßnahmen für die Prozesstechnik-IT ein arbeitsintensiver und langwieriger Prozess ist. Außerdem ist offensichtlich, dass ein ausreichendes Sicherheitsniveau nur erreicht werden kann, wenn die Betreiber von den Anlagen- und Komponentenherstellern die Berücksichtigung grundlegender Sicherheitsprinzipien fordern und die Systeme entsprechend entworfen und implementiert werden. Der hohe Schutzbedarf dieser sensiblen Geschäftsressourcen erfordert hier ein rasches Handeln aller Verantwortlichen.

Referenzen

[1]: Eric Byres, P.E. Joel Carter, Amr Elramly, Dr. Dan Hoffman: „Worlds in Collision - Ethernet and the Factory Floor“

[2]: Eric. J. Byres, P. Eng: „Protect That Network: Designing Secure Networks For Industrial Control“, 2000, IEEE Industrial Applications Magazine

[3]: www.waterisac.org/

[4]: www.bcit.ca/appliedresearch/security/projects/knowledge.shtml

[5]: www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[6]: www.bsi.de/fachthem/kritis/Beispielrichtlinie.pdf

[7]: www.matrikonopc.com/downloads/174/index.aspx

Abkürzungsverzeichnis / Glossar

DCN:	Distributed Control Network
DCS:	Distributed Control System
DMZ:	Demilitarized Zone
ISMS:	Information Security Management System
ISO 27001/ 17799:	Internationale ISO-Standards zu ISMS und Best-Practice Methoden für Informationssicherheit
KRITIS:	Kritische Infrastrukturen
Modbus:	Master/Slave-Kommunikationsprotokoll für PLCs
OPC:	„Openness, Productivity, Collaboration“ (vorher: „OLE for Process Control“), in der Automatisierungstechnik häufig benutzte Software-Schnittstelle, auf DCOM basierend
PCN:	Process Control Network
PIN:	Process Information Network
PLC:	Programmable Logic Controller, elektronische Baugruppe für Steuerungs- und Regelungsaufgaben
RTU:	Remote Terminal Unit
SCADA:	Supervisory Control and Data Acquisition
SPS:	Speicherprogrammierbare Schaltung, siehe PLC
WEP:	Wired Equivalent Privacy, unsicherer WLAN-Verschlüsselungsalgorithmus

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Lokale Netze für Einsteiger, 05.02. - 09.02.07 in Aachen

Dieses 5-tägige Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Preis: € 2.290,- zzgl. MwSt.

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie, 05.02. - 09.02.07 in Aachen

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert. Preis: € 1.690,- zzgl. MwSt.

Windows Vista - Tatsächlich Mehrwerte vorhanden?, 07.02.07 in Köln

Microsoft hat Ende November 2006 die finale Version von Windows Vista freigegeben und stellt diese auch für Unternehmenskunden zur Verfügung. Ende Januar 2007 kommt Vista dann in den Handel. Was haben Unternehmen von dieser neuen Version des führenden Betriebssystems zu halten? Schafft es Microsoft, mit der Etablierung von Vista die Basis für seine „people ready software“ zu legen? Welche Mehrwertpotentiale bietet Vista, insbesondere wenn man schon Windows XP im Unternehmen eingeführt hat?

Preis: € 990,- zzgl. MwSt.

IP-Telefonie evaluieren, planen, betreiben, 12.02. - 14.02.07 in Köln

Dieses 3-tägige Seminar evaluiert Technologien und Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Situation etablierter Hersteller wie Alcatel, Avaya/Tenovis, Cisco, Nortel und Siemens inklusive des Leistungsumfangs ihrer Produkte wird bewertet. Preis: € 1.690,- zzgl. MwSt.

LAN-Praxis-Intensivseminar, 12.02. - 16.02.07 in Aachen

Dieses 5-tägige Intensiv-Seminar trainiert den praktischen Umgang mit geswitchten Ethernet-Netzwerken. Die Teilnehmer bauen aus bereitgestellten Layer-2 und Layer-3-Switch-Systemen, Clienten und Servern Varianten typischer LAN-Designs zusammen. Dabei werden vorgegebene Alltags-Szenerien nachgebildet, auf deren Basis die verschiedenen Konfigurations-Alternativen und Switching-Verfahren durchgespielt werden. Das Seminar geht auf alle typischen Layer-2-/ und Layer-3-Verfahren ein, wiederholt kurz deren Arbeitsweise und vermittelt die optimale Konfiguration. Typische Konfigurationsfehler werden erklärt und anhand vieler Tipps und Tricks aus der Praxis der erfolgreiche Umgang mit einem geswitchten Ethernet trainiert. Preis: € 2.290,- zzgl. MwSt.

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung, 12.02. - 16.02.07 in Aachen

Dieses 5-Tages-Seminar identifiziert die herausragenden Gefahrenbereiche für Firewalls, Webserver, Clienten, Mailsysteme und Netzwerke und zeigt detailliert effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 2.290,- zzgl. MwSt.

Projektmanagement I: Projekte erfolgreich leiten, organisieren und optimieren, 12.02. - 16.02.07 in Aachen

In diesem 5-tägigen Intensiv-Kurs lernen Sie, ein Projekt erfolgreich zu leiten und organisieren. Es werden bewährte Wege aufgezeigt, wie Sie die Projektabwicklung im Alltag in Ihrem Unternehmen konkret optimieren. Preis: € 2.290,- zzgl. MwSt.

Quality of Service - QoS, 12.02. - 13.02.07 in Köln

Dieses 2-tägige Seminar befasst sich mit Quality of Service (QoS) in LAN, WAN und WLAN. Sie lernen, wann QoS erforderlich ist, welche QoS-Standards es gibt, wie eine beherrschbare Architektur aussieht und wie QoS funktioniert. Preis: € 1.390,- zzgl. MwSt.

EMV-gerechte Planung der Elektroinstallation für Rechnerräume und Rechenzentren, 13.02. - 14.02.07 in Bonn

Dieses Seminar zeigt, wie eine EMV-gerechte, hochverfügbare und störungsarme Elektroinstallation mit gleichzeitig hoher Betriebssicherheit geschaffen werden kann. Es vermittelt mit engem Bezug zur Praxis wie ausgehend von Analyse und Messtechnik bestehende Mängel beseitigt werden und ein wartungsoptimierter Betrieb aufgebaut wird. Preis: € 1.390,- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 26.02. - 27.02.07 in Bonn

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes. Preis: € 1.390,- zzgl. MwSt.

Konvergente Netze, 26.02. - 27.02.07 in Bonn

In diesem 3-tägigen Seminar werden sowohl die Einflüsse der Konvergenzfelder und Technologien auf das Design der Unternehmensnetze diskutiert, als auch die Potentiale, die sich daraus ergeben. Preis: € 1.690,- zzgl. MwSt.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
05.02. - 09.02.07 in Aachen
16.04. - 20.04.07 in Aachen
25.06. - 29.06.07 in Aachen
15.10. - 19.10.07 in Aachen
03.12. - 07.12.07 in Aachen

TCP/IP und SNMP
26.02. - 02.03.07 in Berlin
21.05. - 25.05.07 in Aachen
15.10. - 19.10.07 in Berlin

Internetworking
05.03. - 09.03.07 in Aachen
07.05. - 11.05.07 in Aachen
17.09. - 21.09.07 in Aachen
10.12. - 14.12.07 in Aachen

Ethernet Technologien - neuester Stand
26.02. - 02.03.07 in Aachen
21.05. - 25.05.07 in Aachen
10.09. - 14.09.07 in Aachen
26.11. - 30.11.07 in Aachen

Paketpreis für alle vier Seminare € 8.244.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
12.03. - 16.03.07 in Aachen
11.06. - 15.06.07 in Aachen
03.09. - 07.09.07 in Aachen
12.11. - 16.11.07 in Aachen

Trouble Shooting in konvergenten Netzwerken
23.04. - 27.04.07 in Aachen
18.06. - 22.06.07 in Aachen
17.09. - 21.09.07 in Aachen
19.11. - 23.11.07 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
29.01. - 02.02.07 in Aachen
07.05. - 11.05.07 in Aachen
22.10. - 26.10.07 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCSE

ComConsult Certified Security Expert

Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung
12.02. - 16.02.07 in Aachen
18.06. - 22.06.07 in Bonn
10.09. - 14.09.07 in Berlin

Sicherheit 2: VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb
05.03. - 07.03.07 in Bonn
25.06. - 27.06.07 in Berlin
15.10. - 17.10.07 in Aachen

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewall, VPN, Windows-Clienten, WLANs
16.04. - 20.04.07 in Aachen
27.08. - 31.08.07 in Aachen
03.12. - 07.12.07 in Aachen

Paketpreis für alle drei Seminare und Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ € 5.990.-- zzgl. MwSt. (Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.-- / Report 398.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 3234415

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen