Dr. Suppan International Institute

Der Netzwerk Insider

März 2004

Technologie Information für die Ausbildung zum ComConsult Certified Security Expert

Schwerpunktthema

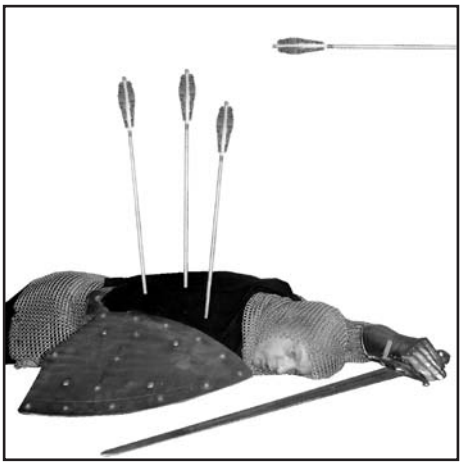
Webanwendungen: Die neue Hintertür ins Unternehmen?

von Detlef Weidenhammer

Immer mehr Unternehmen setzen im Zeitalter des aufkommenden eBusiness verstärkt auf Webanwendungen, um über das Internet Partnern und Kunden einen einfachen Zugriff auf bereit gestellte Geschäftsvorgänge und -daten zu ermöglichen. Dieser Zugriffsweg ist aber auch mit hohen Sicherheitsrisiken verbunden, wie aktuelle Vorkommnisse und die Ergebnisse von Sicherheitsüberprüfungen deutlich zeigen.

In diesem Beitrag werden typische Schwachstellen von Webanwendungen aufgezeigt und Schutzmaßnahmen von der Programmierung bis zum Betrieb vorgestellt.

Webanwendungen sind technisch gesehen Client/Server-Anwendungen, die über das Transportprotokoll HTTP eine Interaktion zwischen Unternehmen oder von Unternehmen zu Kunden realisieren. Den Möglichkeiten einer Webanwendung sind dabei kaum Grenzen gesetzt. Diese reichen von der einfachen Recherche in lokalen Dateiverzechnissen bis hin zu den komplexen Funktionen eines Online-Sales oder Online-Bankings. Wurden zunächst vorwiegend einfache CGI-Anwendungen implementiert, die auf dem Webserver selber abliefen, so basieren heutige Webanwendungen zumeist auf Java und laufen verteilt auf mehreren Servern. Eine strenge Definition des Begriffs Webanwendung gibt es bisher nicht, üblicherweise versteht man darunter Anwendungen, die zumindest 3-stufig mit Presentation-, Application- und Data-Layer aufgebaut sind und über HTTP mit einem Anwender oder einer anderen Webanwendung kommunizieren. In diesem Sinne zählen auch Webportale und Web-Services dazu. Die in diesem Beitrag angesprochenen Sicherheitsprobleme sind weitgehend identisch, auf deutliche Unterschiede wird hingewiesen.



Trefferquote 3 von 4
bei Angriff durch die Hintertür

weiter Seite 16

Zweitthema

Voice-over-IP Lösungen und Sicherheit

von Dipl.-Inform. Petra Borowka

Seit der Vermarktung von IP Telefonie wird als wesentliche Hemmschwelle für deren Einsatz immer wieder der Sicherheitsaspekt genannt. Wo liegen die Risikopotenziale? Was tun die Hersteller und Standardisierer zur Verbesserung? Wie lassen sich VoIP Lösungen sicher machen?

Dieser Beitrag setzt ein grundsätzliches Verständnis voraus, wie IP Telefonie funktioniert und welche Protokolle und Verfahren hier zum Einsatz kommen. Für eine Einführung in Voice over IP verweisen wir auf die Netzwerk Insider vom September und November 2000:

"Quo vadis, VoIP? Der Voice-Markt ist da – aber wo läuft er hin?"

"Quo vadis, VoIP? Der Voice-Markt ist da – was tun die Hersteller?"

weiter Seite 6

Neue Zertifizierung

C³sec: ComConsult Certified Security

auf Seite 13

Zum Geleit

Webanwendungen: Schlüssel-Technologie für das Redesign unserer Netzwerke und DV-Architekturen

auf Seite 2

Zum Geleit

Webanwendungen: Schlüssel-Technologie für das Redesign unserer Netzwerke und DV-Architekturen

Webanwendungen gelten innerhalb der Unternehmen als der Schlüssel zur Umsetzung neuer Prozess-Abläufe. Gleichzeitig versprechen sie eine drastische Verringerung der Entwicklungs- und Pflegekosten. Doch viele dieser Entwicklungen werden schon fast naiv umgesetzt. Typische Beispiele wie das Portal der Bundesanstalt für Arbeit zeigen, wie leicht man die Herausforderungen einer neuen Technologie unterschätzen kann. Eine wesentliche Dimension der Umsetzung von Webanwendungen ist dabei ohne Zweifel der Bereich der Daten- und Sabotage-Sicherheit. Der Leitartikel dieser Ausgabe des Insiders belegt in beeindruckender Form die Gefahren, die hier bestehen. Eine 75%-Erfolgsquote im Angriff auf Webanwendungen kann nur als Desaster bezeichnet werden.

Kern aller Webanwendungen ist der Begriff der IP-Realzeit-Kommunikation. Auf der Basis einer flächendeckenden Verfügbarkeit von IP-Netzwerken können Mitarbeiter an jedem Ort in Realzeit in die wichtigen Geschäftsprozesse eines Unternehmens einbezogen werden. Aktuelle Studien von Roland Berger und Siemens belegen die wirtschaftlichen und organisatorischen Vorteile, die damit speziell in den Bereichen Vertrieb, Post-Sales-Support und Kundenservice erreicht werden können. Immer mehr Technologien richten sich an dieser neuen Vision aus. Der neueste Trend ist die Einbeziehung der Sprachkommunikation in diese Welt. Alle für den Markt wesentlichen TK-Anbieter forcieren speziell diesen Gesichtspunkt. Auf dem deutschen Markt ist dies sehr gut im Wettbewerb zwischen Cisco und Siemens um die beste TK-Lösung auf der Basis IP-Telefonie zu beobachten (siehe dazu unsere aktuelle Studie: Cisco versus Siemens: wer hat die bessere TK-Lösung).

Es zeigt sich aber immer mehr, dass unsere bestehenden Netzwerk- und IT-Infrastrukturen dieser Entwicklung nur bedingt gewachsen sind. Die immer weitere Ausdehnung der IP-Verfügbarkeit (typisch durch Wireless LAN´s), die Einbeziehung immer neuer Benutzgruppen in unsere Netzwerke, die zunehmende Schaffung neuer Anwendungen auf dieser Basis überfordern unsere Infrastrukturen.

Im Gegensatz zu früheren Zeiten ist dies keine kapazitive sondern eine funktionale Überforderung, auch wenn gerade im Rechenzentrum an Anpassung der Kapazitäten an den zunehmenden Trend der Zentralisierung bei gleichzeitiger Globalisierung dringend erforderlich ist (typisch: mehrere Rechenzentren ergänzen sich zur globalen Abdeckung mit Desaster Recovery Funktionalität).

Die Schlüsselthemen für den Erfolg der neuen Projekte und Nutzungsformen sind Sicherheit und Benutzertrennung im Netzwerk. Im Bereich Sicherheit zeigt der Leitartikel die gesamte Tragweite der Problematik auf. Er weist aber auch gleichzeitig die Lösbarkeit durch geeignete Architekturen nach. Im Bereich Benutzertrennung kennzeichnet die Diskussion über Verzeichnisdienste und die Einbindung von Authentifizierung und Zertifikatsverwaltung die aktuelle Diskussion.

Vereinfacht ausgedrückt sind die Unternehmen gefordert, zuerst ein tragfähiges Fundament zu schaffen bevor sie immer weitere Projekte mit immer neueren Technologien in die bestehenden Infrastrukturen integrieren. Dieses wird häufig vernachlässigt. Dazu gibt es unzählige Beispiele. Wie viele Unternehmen nehmen Wireless-Technologien in Betrieb, ohne vorher über eine generelle Architektur für WLAN´s nachgedacht zu haben? Wie viele Unternehmen fangen in der Fertigung an, Ethernet immer näher an den Produktionsprozess zu bringen ohne vorher ein Rahmenkonzept entwickelt zu haben? Wie viele Unternehmen dehnen ihre IP-Infrastrukturen immer weiter aus, ohne dabei den Umfang und die Qualität des IP-Managments ebenfalls auszubauen? Wie viele Unternehmen führen Linux parallel zu Windows ein ohne dabei eine übergeordnete Benutzer- und Verzeichnisverwaltung zu realisieren?

Das Redesign bestehender Netzwerk- und IT-Architekturen ist das Gebot der Stunde. Wir helfen Ihnen dabei:

- das IT-Sicherheitsforum 2004 ist die ideale Veranstaltung, um auf hochaktuellen Niveau das Thema Sicherheit unter den Rahmenbedingungen neuer IT-Anforderungen zu diskutieren und entsprechende Lösungsansätze kennen zu lernen ("ComConsult IT-Sicherheits-Forum 2004" ab Seite 4)

- unser Seminar DNS/DHCP/NAT führt in die moderne Form des IP-Managements ein ("DNS / DHCP / NAT: IP-Infrastrukturdienste optimal einsetzen und Zusatzpotenziale nutzen" auf Seite 3)

- unser Seminar über WLAN-Technologien zeigt, wie eine tragfähige Infrastruktur für Wireless-Technologien entsteht (Wireless LAN Grundlagen: Planung, Produktauswahl, Installation, Trouble Shooting auf Seite 3)

- unser Seminar über J2EE zeigt, was moderne Applikationen und Architekturen leisten ("Umsetzung neuer System-Architekturen mit J2EE, XML und Web-Services: welche Plattform ist die „richtige“?" auf Seite 3)

- unser brandneuer und Top-aktueller Report über Ethernet in der Produktion zeigt, wie ein sinnvolles und tragfähiges Rahmenkonzept für Ethernet in der Produktion auch unter Berücksichtigung von Sicherheits-Anforderungen entsteht ("Ethernet in der Industrie" auf Seite 3)

Ich freue mich darauf, diese Themen in den nächsten Monaten verstärkt mit Ihnen diskutieren zu können.

Ihr Dr. Jürgen Suppan

DNS / DHCP / NAT: IP-Infrastrukturdienste optimal einsetzen und Zusatzpotenziale nutzen

Seminar

04.10. - 06.10.04 Bonn

Dieses Seminar vermittelt, wie DNS, DHCP und NAT arbeiten und wie eine professionelle Umsetzung aussieht.
Dabei wird im Detail auf die Varianten der Verfahren eingegangen und das damit verbundene Potenzial aufgezeigt.

Referent: Markus Schaub
Preis: € 1.690,-- zzgl. MwSt.

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

Wireless LAN Grundlagen: Planung, Produktauswahl, Installation, Trouble Shooting

Seminar

03.05. - 05.05.04 Zürich
14.06. - 18.06.04 Bonn

Dieses Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur.

Referenten: Dr. Simon Hoff, Dr. Ing. Joachim Wetzlar
Preis: € 1.690,-- zzgl. MwSt.
als 5-tägiges Seminar mit Vertiefung: € 2.290,-- zzgl. MwSt.

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

Umsetzung neuer System-Architekturen mit J2EE, XML und Web-Services: welche Plattform ist die „richtige“?

Seminar

21.06. - 23.06.04 Bonn

Dieses Seminar gibt einen Überblick über die verfügbaren Technologien, analysiert ihre Nutzbarkeit und ordnet sie in den aktuellen Entwicklungstrend im Sinne der Entscheidung für die „richtige“ Technologie ein.

Referenten: Dipl.-Ing. Christian Roszak, Dr. Ralf Altmeyer
Preis: € 1.690,-- zzgl. MwSt.

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

Ethernet in der Industrie

Der Report analysiert die bestehenden Aufgaben, bewertet die notwendigen Eigenschaften von Komponenten und erarbeitet einen neuen Design-Rahmen für Ethernet in der Industrie. HINDA ist das neue Schlagwort des Jahres 2004: Hierarchical Industrial Network Design and Architecture.

Preis: € 398,-- zzgl MwSt.

Bestellen Sie über unsere Web-Seite
www.comconsult-research.com

Aktueller Kongress

IT-Sicherheits-Forum 2004

IT-Sicherheit in Theorie und Praxis – Die wichtigsten Entwicklungen bei Bedrohungen und Schutzmaßnahmen

Vom 10. bis 13. Mai veranstaltet die ComConsult Akademie im Maritim Hotel Königswinter das IT-Sicherheits-Forum Forum 2004.

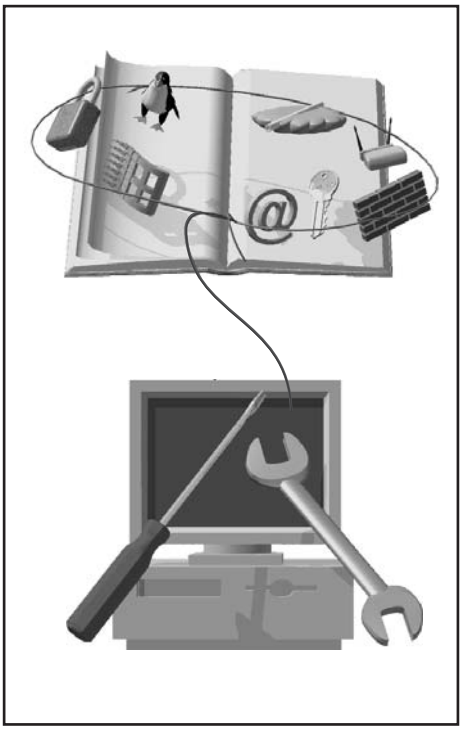
Das Programm aus Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und Angriffssimulationen verbindet die Vermittlung aktuellen Knowhows mit der im Tagesbetrieb benötigten Praxisrelevanz. Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei Tutorien (IT-Sicherheit im Überblick, zwei Fachthemen). Als Schwerpunkte sind in diesem Jahr vorgesehen:

- Webanwendungen mit gravierenden Risiken
- Content-Security: Umgang mit gefährlichen Inhalten
- Erweiterte Sicherung der Netzgrenzen
- Mobility unter Sicherheitsaspekten
- Zentrale Mailverschlüsselung
- Patch- und Updatemanagement
- Sicherheitsstrukturen für interner Netze
- Sicherung von WLANs
- Intrusion Detection / Intrusion Prevention
- Auditierung und Zertifizierung
- Praxis-Workshops

Einige Themenschwerpunkte des ComConsult IT-Sicherheits-Forums im Detail:

Webanwendungen mit gravierenden Risiken

Mit der zunehmenden Bereitstellung von Webanwendungen, die über das Internet einen einfachen Zugriff auf bereit gestellte Geschäftsvorgänge und Daten eines Unternehmens ermöglichen, sind auch hohe Sicherheitsrisiken verbunden. Schutzmaßnahmen mit Firewalls haben ihre Stärken in der Kontrolle auf Netzebene, können aber auf Anwendungsebene bestenfalls offensichtlichen Missbrauch erkennen. Angriffe neuerer Art zielen aber eher auf Schwachstellen innerhalb einer Anwendung. Ursache hierfür ist zumeist die mangelhafte Beachtung von Sicherheitsaspekten bei der Programmierung. Im Forum werden aktuelle Angriffe auf Webanwendungen und Web Services gezeigt und erläutert. Schutzmaßnahmen werden von der Programmierung bis zum Betrieb aufgezeigt.



Content-Security: Umgang mit gefährlichen Inhalten

Die meisten Unternehmen schenken heute den Sicherungsmaßnahmen an ihren Netzgrenzen, insbesondere zum Internet, eine hohe Aufmerksamkeit. Security-Gateways wie Firewalls oder RAS-Server überwachen Verbindungen und sollen bösartige Zugriffe abwehren. Bei fachgerechtem Betrieb und Einsatz in aktueller Version wird damit auch für versierte Angreifer ein Erfolg immer schwieriger. Eine viel größere Gefahr wird aber von den meisten Unternehmen stark unterschätzt. Angriffsformen, die sich in transferierten Daten z.B. bei Web- oder Mailverkehr verbergen, stellen mittlerweile eine der größten Bedrohungen dar. Je nach Intention der Angreifer lassen sich sogar interne Systeme massiv stören, Nutzerberechtigungen übernehmen oder gezielt gesuchte, vertrauliche Daten ausspähen. Im Forum wird neben den Themen "Kontrolle von Webinhalten" und "Zentrales Management" insbesondere die Gefahr durch neuartige multifunktionale Würmer thematisiert.

Erweiterte Sicherung von Netzgrenzen

Die gute Sicherung der Netzgrenzen eines Unternehmens (der Perimeter) umfasst weit mehr als den Einsatz von Internet-Firewalls und Anti-Viren Lösungen. Die zunehmende Vernetzung zwischen Partnern im eBusiness und der Einsatz von unterschiedlichen Techniken für Fernzugriffe bei VPN/RAS-Lösungen öffnen neue Zugangswege mit beträchtlichen Risiken. Im Forum wird aufgezeigt, wie solche Verbindungen zu sichern sind und welche Gefahren bei unzureichender Administration der DMZ oder der „inbound"-, „outbound"-Verbindungen drohen.

Mobility unter Sicherheitsaspekten

Mobile Geräte spielen eine immer größere Rolle in der Arbeitsumgebung und müssen aus Sicherheitssicht besonders kritisch beachtet werden. Fehlende Kenntnis über die mit ihrem Betrieb verbundenen Gefahren führt in den meisten Unternehmen zu einer völligen Unterschätzung der Sicherheitsrisiken. Im Forum werden die unterschiedlichsten mobilen Geräte (Notebook, PDA, MDA, Handy) und eingesetzten Techniken (Bluetooth, WLAN, IrDA) vorgestellt, unter Sicherheitsaspekten bewertet und mit Empfehlungen versehen.

Zentrale Mailverschlüsselung

Dass E-Mail für die meisten Unternehmen mittlerweile zu einem unverzichtbaren Kommunikationsmittel geworden ist, ist hinlänglich bekannt. Auch der mangelhafte Schutz von E-Mails gegen Mitlesen und Manipulation sollte jedem Sicherheitsinteressierten bewusst sein. Im eklatanten Widerspruch dazu steht, dass die wenigsten Firmen über E-Mail-Verschlüsselungslösungen verfügen. Die meist genannten Gründe dafür sind hohe Kosten und die Komplexität der Einführung von Client-basierenden Lösungen. Neuere Ansätze gehen daher dazu über, zentrale Kryptogateways einzusetzen und erfordern weder Kryptosoftware am Desktop noch müssen die Mitarbeiter aufwändig in die Benutzung der Software eingeführt werden. Im Forum werden zentrale Mail-Gateways für die Signierung und Verschlüsselung vorgestellt und deren Vor- und Nachteile im Betrieb erläutert.

ComConsult IT-Sicherheits-Forum 2004

Patch- und Updatemanagement

Bis vor wenigen Jahren war Patchmanagement kein wirklich relevantes Thema für Administratoren und Sicherheitsverantwortliche. Zumeist wurden nach der Installation eines Systems Patches selten oder gar nicht installiert. Insbesondere im letzten Jahr führten die durch Internet-Würmer wie Slammer, Blaster und Nachi verursachten Schäden aber auch einer breiten Öffentlichkeit vor Augen, dass die regelmäßige unternehmensweite Installation von Patches essentiell für einen sicheren und störungsfreien IT-Betrieb ist. Neben Betriebshinweisen werden auf dem Forum auch einige hilfreiche Tools vorgestellt und bewertet.

Neben diesen Schwerpunkten sind weitere Beiträge zu folgenden Themen geplant:

Sicherheitsstrukturen für interner Netze

Der Betrieb transparenter Netzwerke, die keine interne Sicherheitsstrukturierung aufweisen, lässt sich aus heutiger Sicht nicht mehr vertreten. Es werden Konzepte zum Aufbau einer sicherheitssegmentierten Umgebung vorgestellt.

Sicherung von WLANs

Darstellung von Sicherheitsstandards im WLAN-Bereich. Konzepte für „offene“ und „geschirmte“ WLANs unter Einbeziehung interner und externer Nutzergruppen.

Intrusion Detection/Intrusion Prevention

Einsatzmöglichkeiten und –grenzen von kommerziellen und freien Intrusion Detection und Intrusion Prevention Systemen. Integration in das Sicherheitsmanagement.

Auditierung und Zertifizierung

Mit Auditierungen und Zertifizierungen nach BSI Grundschutz und nach BS 7799 liegen nun endlich auch in Deutschland erste Erfahrungen vor. Auf dem Forum werden Praxisberichte über Erfahrungen bei der Anwendung dieser Vorgehensweisen wird auf dem Forum berichten.

Praxis-Workshops

Am 3. Tag werden in parallelen Sessions stark praxisorientierte Workshops durchgeführt. Dazu gehören moderierte Produktvergleiche (u.a. zu IDS/IPS, Application Shields, eMail Kryptogateways, Log- und Alarmlösungen) ebenso wie die gemeinsame Erarbeitung von Lösungsszenarien (u.a. für WLAN, Sicherheitsorganisation, Perimetersicherung).

10 % Frühbucherrabatt bis 31.03.04

IT-Sicherheits-Forum 2004

10.05. - 13.05.04 in Königswinter

4 Tage IT-Sicherheits-Forum 2004 mit Tutorium zum Preis von € 1.750,-- statt regulär € 1.990,-- zzgl. MwSt.

3 Tage IT-Sicherheits-Forum 2004 ohne Tutorium zum Preis von € 1.485.-- statt regulär € 1.690,-- zzgl. MwSt.

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Kongress-Anmeldung

Ich melde mich an für das
ComConsult IT-Sicherheits-Forum 2004

☐ **vom 10.05. - 13.05.04 mit Tutorium**
zum Preis von € 1.750,-- zzgl. MwSt.*

☐ **vom 11.05. - 13.05.04 ohne Tutorium**
zum Preis von € 1.485,-- zzgl. MwSt.*

*Frühbucherpreise gültig bis 31.03.04

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Zweitthema

Voice-over-IP Lösungen und Sicherheit

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka hat langjährige Praxis-erfahrung mit mehr als 15 Jahren herstellerneutraler Netzwerkplanung in Projekten für verschiedenste Industrie- und Dienstleistungsunternehmen; bekannt durch viele Schulungen und Veröffentlichungen. Sie leitet das Planungsbüro Unternehmensberatung Netzwerke UBN in Aachen.

Sicherheit in klassischen TK-Netzen

Klassische TK-Netze (TDM Telefonie) arbeiten verbindungsorientiert, d.h. vor dem Übertragen des ersten Datenbits wird eine feste Verbindung aufgebaut und in der Verbindungsaufbauphase können Sicherheitsmechanismen aktiviert werden. Klassische TK nutzt die so genannte Outband Signalisierung, d.h. Zugriff auf den Nutzdatenkanal bedeutet noch nicht, Zugriff auf den Steuerungskanal zu haben.

Broadcast- und Multicast-Mechanismen fehlen, daher ist das Verzweigen und Kopieren eines Datenstroms schwierig und das Ablauschen einer einzelnen Verbindung ist bei der existierenden Vielzahl von Verbindungen relativ aufwendig.

Aufgrund der proprietären Steuerungs-Software sowie der Nutzung proprietärer Betriebssysteme liegt das Hacken von TK-Switches nicht im Fokus von Teenager-Hackern.

Der Angriffsbereich klassischer TK-Netze befindet sich eher im Betrug bei der Nutzung von TK-Diensten (toll fraud), bei dem der Angreifer das TK-Equipment eines Dritten nutzt, um auf fremde Rechnung selbst kostenlos zu telefonieren.

Sicherheit in IP-Netzen

IP-Netze arbeiten verbindungslos, jedes System kann jedem anderen System Pakete schicken. Lediglich wenn auf der Transportschicht das verbindungsorientierte TCP genutzt wird, können beim Verbindungaufbau Sicherheitsmechanismen aktiviert werden. Realzeit-Protokolle wie RTP nutzen jedoch anstelle von TCP das verbindungslose UDP.

IP-Netze verwenden Inband Signalisierung und Session Hijacking ist ein bekanntes Beispiel dafür, dass die übermittelten Steuerinformationen manipuliert werden können.

Aufgrund der genutzten Broadcast-Mechanismen ist das Abhören von Informationen, die weitergehende Angriffe ermöglichen, einfacher als bei TDM-Telefonie. Aufgrund der unterstützten Multicast-Technik ist das Verzweigen und Kopieren von Informationen möglich.

Die genutzten Standard-Betriebssysteme für Anwendungs- / TK-Server machen diese zum Angriffspotenzial vieler Hacker.

Seminar zum Thema

IP-Telefonie: evaluieren, planen, betreiben

Seminar

24. - 26.05.04 Köln

27. - 29.09.04 Bonn

Dieses Seminar evaluiert die Technologie und die verfügbaren Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung.

Referent: Referentin: Dipl.-Inform. Petra Borowka
Preis: € 1.690,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Voice-over-IP Lösungen und Sicherheit

Wo liegen Bedrohungspotenziale für VoIP Lösungen und wie sind sie einzuordnen?

Schlagzeilen wie "Voice over IP Netze sind durch Sicherheitslöcher in den Standard-Protokollen Attacken ausgesetzt", "Neue Sicherheitslücken in Windows und Linux entdeckt" untermauerten im Januar 2004 ein weiteres Mal die Skepsis der Skeptiker und Zögerlichkeit der Vorsichtigen.

Machten in 2003 noch SIP-Sicherheitslücken bei zehn getesteten Herstellern Furore, was mit dem Argument "junge Implementierung" beschwichtigt wurde, so ging im Januar 2004 die Verwundbarkeit für DOS Attacken von H.323 bei marktführenden Firmen wie Microsoft (Internet Security and Acceleration Server) und Cisco (H.323 im Cisco IOS, IOS Firewall, Cisco Director Agent auf IBM Servern mit speziellen TCP / UDP Ports) durch die Medien.

Leider konnte hier nicht dieselbe Beschwichtigung verwendet werden, da H.323 schon ein Alter von fünf Jahren überschritten hat...

Betrachten wir denkbare Angriffsszenarien bei dem neuen Standard SIP, der sich für den Zugang von Privaten zu öffentlichen Netzen in den nächsten Jahren zunehmend durchsetzen wird:

- Registration Hijacking: Ein Angreifer gibt sich als "ordentlicher" Benutzer aus, führt die Registrierung unter falschem Namen durch und nimmt somit die Identität des Benutzers an (Abhilfe: Client Authentifizierung)
- Server Spoofing: Ein Angreifer nimmt die Funktion eines SIP Servers an und leitet SIP Requests so um dass sie mitgelesen werden können oder "verschwinden" (Abhilfe: Server Authentifizierung)
- Eine SIP Session wird abgehört (Abhilfe: Verschlüsselung)
- Von einem Angreifer eingespielte SIP Meldungen können zu Denial of Service führen

Tatsache ist:

Beim Umstieg von klassischer TK auf Voice over IP darf der Betreiber nicht nur die Invest- und Betriebsvorteile im Blick haben, sondern muss sich auch verschärft Gedanken über ein schlüssiges Sicherheitskonzept machen.

Hierzu gehören mehrere Schritte:

Schritt 1

Risikoabschätzung: Wie groß ist die Angst vor einer Bedrohung, wie wahrscheinlich ist ein Angriff, welcher Schaden kann entstehen?

Schritt 2

Definition 1: Welche Anwendungen / Dienste, Komponenten und Netzbereiche sollen geschützt werden? Mit welchem finanziellen und betrieblichen Aufwand?

Schritt 3

Definition 2: Wogegen soll der Schutz erfolgen? DOS, Theft of Service, Manipulation, administrative Übernahme?

Schritt 4

Definition 3: Welche Schutzmaßnahmen sollen durchgeführt werden?

Schritt 5

Implementierung und Test der Schutzmaßnahmen

Schritt 6

Permanentüberwachung und intervallmäßige Audits zum Auffinden von Schwachstellen

Schritt 1

Beseitigen gefundener Schwachstellen: rekursiv ab Schritt 1

Wir werden uns in diesem Beitrag auf die zu schützenden Bereiche sowie mögliche Schutzfunktionen und –maßnahmen konzentrieren. Die schützenswerten Bereiche gliedern sich ähnlich wie in jedem vernetzten Anwendungs-Szenario:

- TK-Applikationsserver
- TK-Server
- Gateways
- TK-Endgeräte
- VoIP Netzwerk: Protokolle, Netzkomponenten

Report zum Thema

Voice over IP:

Anforderungs-katalog und Evaluierung

Dieser Report setzt sich kritisch mit dem Thema Voice over IP auseinander und stellt die Fragen nach Leistungsmerkmalen, Sicherheit, Verfügbarkeit und Skalierbarkeit der Produkte wichtiger Hersteller wie Avaya, Alcatel, CISCO, Nortel und Siemens und gibt Kriterien, wann ein Einsatz sinnvoll ist und wann man mit seiner Entscheidung noch warten sollte.

Voice over IP Report
Februar 2003
275 Seiten
Preis: € 398,-- zzgl MwSt.

Bestellen Sie auf unserer Web-Seite
www.comconsult-research.com

TK-Server,
TK-Applikationsserver

Hinsichtlich der TK-Server bestehen die größten Sicherheitsbedenken weniger gegenüber einem Ablauschen von Gesprächsinhalten als gegenüber einem Denial of Service (DOS) oder der Möglichkeit, dass ein Angreifer die administrative Kontrolle über den Server erhält. "Unser XXX TK-Server wurde vom Slammer Virus lahm gelegt", sagt der Technische Leiter einer amerikanischen Kreuzfahrt-Gesellschaft. "Es war eine Demobox, und auf die waren die aktuellen Viruspatches nicht mit aufgespielt worden". Glücklicherweise war die XXX IP PBX auf Basis eines Windows Servers nur zur Evaluierung im Einsatz. Das System, das sich jetzt im Produktivbetrieb befindet, erhält alle Patches, wird überwacht und regelmäßig hinsichtlich Security-Updates und Patches gewartet.

Grundsätzlich ist davon auszugehen, dass TK-Server mit einem proprietären Betriebssystem (RMX, VxWorks o.ä.) weniger Angriffen ausgesetzt sind als TK-Server mit einem Standard-Betriebssystem (Windows, Linux, Unix), da es sehr viel weniger Know How über proprietäre Systeme gibt und die Summe erreichbarer Server hier erheblich kleiner (also für Angreifer "weniger lohnend") ist. Insofern sind aus Sicherheitsgründen proprietäre Systeme zu bevorzugen. Demgegenüber steht jedoch der Nachteil, dass für solche Systeme insgesamt weniger Know How, weniger Anwendungen und weniger Entwicklungs-Flexibilität gegeben ist. Der Trend im TK-Markt geht entsprechend in die Richtung, TK-Software auf der Basis von Standard-Servern (IBM, Sun, HP) und Standard-Betriebssystemen (Linux, Windows, seltener Unix) einzusetzen.

Soll als TK-Server ein Standard-Server mit Standard-Betriebssystem eingesetzt werden, so sind einige Punkte zu beachten, auf die wir nachfolgend eingehen.

- Default Passwörter müssen sofort geändert werden, die Gültigkeit eines Passwortes darf nicht zu lang sein.
- Alle nicht benötigten Dienste und Systemprozesse müssen deaktiviert werden, nicht benötigte TCP / UDP Portnummern (Listening Sockets) deaktiviert und gesperrt werden, z. B. insbesondere RIP, NFS, SMB, X-windows, rcp, rsh, rlogin, rexec. Avaya hat dies bei der Systemauslieferung als "hardened" Linux so eingestellt, Cisco ermöglicht eine Festlegung der erlaubten und nicht erlaubten Systemaktionen über den Cisco Security Agent (CSA).
- Datei- und Verzeichniszugriffsrechte müssen soweit wie möglich eingeschränkt werden.
- Bei Inaktivität sollte nach kurzer Zeit ein Logoff erfolgen.
- Verschlüsselung des Management-Zugriffs mit HTTPS, SSH oder SNMPv3 sind notwendig.
- Authentifizierung für den Management-Zugriff ist zu fordern, Optionale One-Time Passwörter sind wünschenswert.
- Remote Login muss in der Form steuerbar sein, dass eingehende Einwahl geblockt oder auf einen Einzelzugriff beschränkt werden kann.
- Das TK-Administrator Login sollte nicht automatisch die Root Rechte und den Shell Zugriff für das Betriebssystem beinhalten.
- Zum Schutz gegen Viren sind entsprechende Virenscanner einzusetzen. Hier entsteht das Problem, dass teilweise der aktuellste Virenscanner nicht für das per Auslieferung des TK-Servers "eingefrorene" Betriebssystem freigegeben ist.
- Eine weitere Hilfe sind Intrusion Detection Systeme (IDS) und seit kurzem Intrusion Protection Systeme (IPS), die dynamisch anhand von ungewöhnlichen Zugriffsmustern noch unbekannte Angriffe erkennen und unterdrücken sollen. Cisco vermarktet hier den Cisco Security Agent, der einerseits ermöglicht, alle Systemaktionen als erlaubt oder unerlaubt zu konfigurieren und andererseits ungewöhnliche Zugriffsmuster als potenziellen Angriff erkennen und blockieren soll.
- Darüber hinaus sollte auf dem TK-Server Überwachung und Protokollierung aller erlaubten und insbesondere aller unerlaubten Zugriffe erfolgen.
- Die Unterstützung und Nutzung separater Ethernet Schnittstellen und separater VLANs für Administration einerseits und die produktive Verbindung zwischen TK-Server und Clients anderer-seits bietet zusätzliche Sicherheit und Abschottung.

Seminar zum Thema

IP-Telefonie: Projektleitfaden

Seminar

15. - 17.03.04 Düsseldorf
03. - 05.05.04 Zürich
21. - 23.06.04 Berlin

Dieses Seminar erarbeitet einen Leitfaden zur Umsetzung von IP-Telefonie in der Praxis. Alternativen werden verglichen, bekannte Probleme aufgezeigt, erfolgreiche Konzepte vermittelt.

Referent: Dr. Behrooz Moayeri (ComConsult Beratung und Planung)
Preis: € 1.690,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Gateways

Die Sicherheitsbedenken bei Gateways sind ähnlich gelagert wie bei einem TK-Server, wobei das typische Gateway von zwei Seiten aus angreifbar ist, über das IP Netzwerk und über das PSTN-Netzwerk.

Wie beim Serverbetrieb sind auch beim Gatewaybetrieb Maßnahmen für den Zugriffsschutz zu treffen:

- Default Passwörter müssen sofort geändert werden, die Gültigkeit eines Passwortes darf nicht zu lang sein.
- Nicht benötigte Dienste und Systemprozesse müssen deaktiviert werden, nicht benötigte TCP / UDP Portnummern (Listening Sockets) deaktiviert und gesperrt werden.
- Zugriffsrechte müssen soweit wie möglich eingeschränkt werden.
- Ab einer bestimmten Anzahl erfolgloser Login-Versuche innerhalb einer bestimmten Zeit sollte ein Lock out des Benutzers erfolgen.
- Verschlüsselung des Management-Zugriffs mit HTTPS, SSH oder SNMPv3 sind notwendig.
- Authentifizierung für den Management-Zugriff ist zu fordern, Optionale One-Time Passwörter sind wünschenswert.
- Remote Login muss in der Form steuerbar sein, dass eingehende Einwahl geblockt oder auf einen Einzelzugriff beschränkt werden kann.

Da Gateways die Verbindungsfunktionalität zum PSTN-Netzwerk bereitstellen, besteht ein weiteres Sicherheitsrisiko im toll fraud, der Nutzung des PSTN-Zugangs durch unbefugte Dritte. Anzeichen für toll fraud ist insbesondere gegeben, wenn

- überdurchschnittlich lange Holdtimes auftreten
- die Gateway-Nutzung von befugten Benutzern ungewöhnlich lange Antwortzeiten zeigt
- die Anzahl der Anrufe außerhalb der normalen Geschäftszeiten sprunghaft ansteigt
- ungewöhnliche Anwahlnummern auftauchen

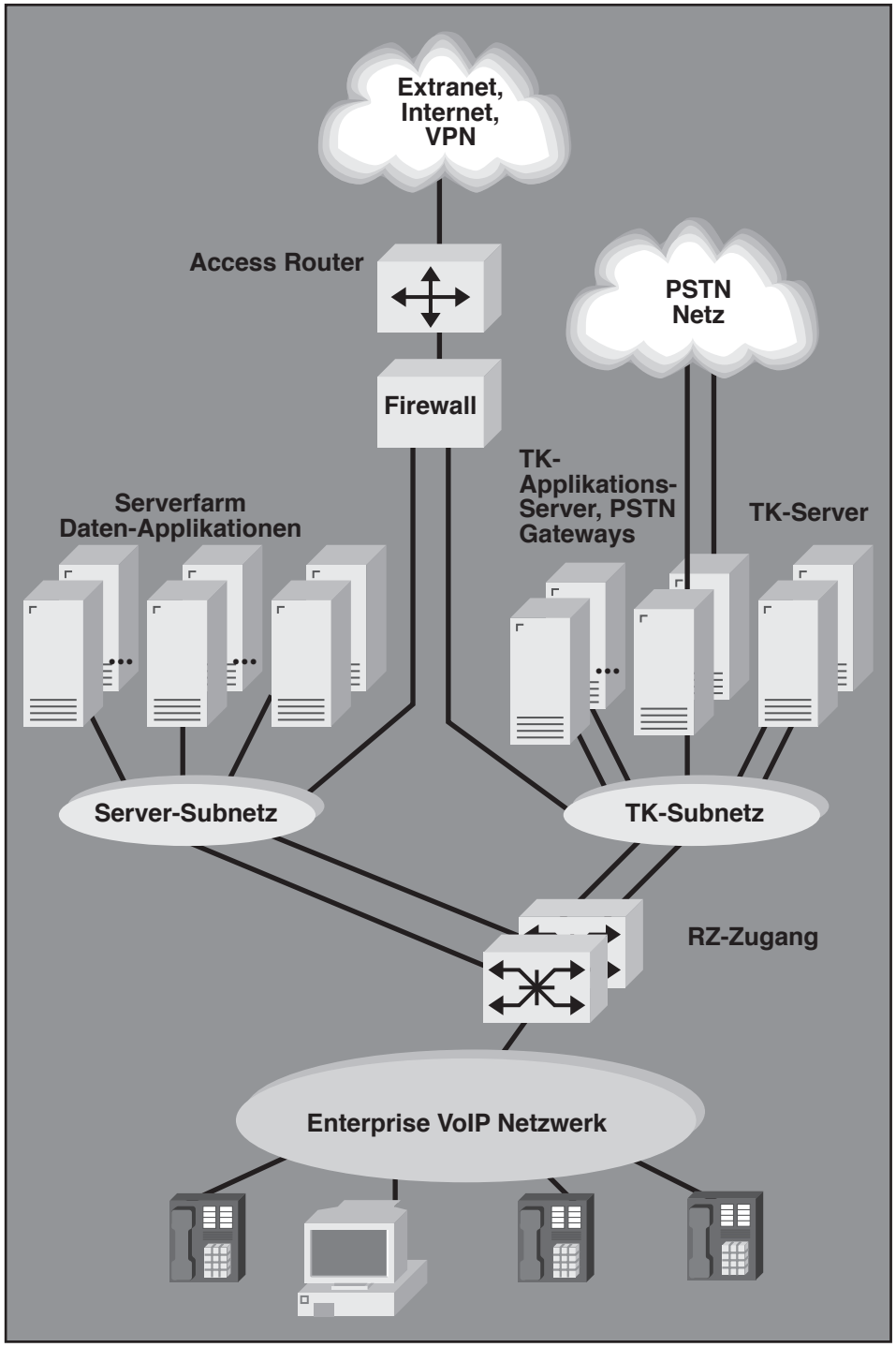


Bild 1: Positionierung von TK-Servern und PSTN-Gateways im Enterprise Netzwerk

Sowohl für TK-Server als auch für Gateways macht es Sinn, diese Systeme zum Schutz gegen Angriffe aus externen Netzen in einer separaten DMZ mit Firewall-Abkopplung zu positionieren. Der erreichbare Schutz ist nochmals verbessert, wenn in dieser DMZ keinerlei andere Server und Dienste verfügbar (und somit auch nicht hackbar) sind. Da für Telefonie die Datenraten nicht sehr hoch sind, kann für die betreffenden Firewalls das Hauptaugenmerk auf die Funktion "Abwehr von DoS Attacken" gelegt und der erreichbare Durchsatz als sekundär betrachtet werden.

TK-Endgeräte

Ähnlich wie bei Wireless LAN wird beim einzelnen TK-Endgerät, z.B. IP-fähiger Handapparat mit Ethernet oder WLAN Anschluss, Softphone, PDA etc., das Risiko eines DOS Angriffs oft als relativ niedrig eingeschätzt, das Risiko, dass ein Gespräch mitgeschnitten oder abgelauscht wird, jedoch als hoch bewertet. Die Standardisierung bei der IETF trägt dieser Sicherheitslücke mit der Entwicklung von RTPS Rechnung, einer verschlüsselten Version des RTP (siehe Bild 2). Zum Schutz gegen unbefugten Netzzugang, also auch Nutzung eines Telefons, wurde seitens der IEEE der LAN Standard IEEE 802.1X (Port Security) verabschiedet, der EAP zwischen Endgerät und Switch sowie z.B. RADIUS zwischen Switch und Authentifizierungs-Server zur Authentifizierung eines Endgeräts beim LAN-Zugang definiert. Ein Angreifer, der sich an einen internen LAN-Port anschaltet, hätte somit keine Möglichkeit, ins Netz zu kommen, da er am ersten LAN Switch bei der Authentifizierung scheitert. Allerdings ist der Standard 802.1X bei Telefonen nur bedingt wirksam, da das Telefon üblicherweise permanent aktiv, also eingeloggt ist und im Gegensatz zum PC oder Laptop nicht jeden Morgen neu gebootet wird.

Hersteller wie Avaya (Communication Manager v2.0) oder Cisco (Call Manager v4) warten jedoch nicht bis zur Fertigstellung von RTPS sondern gehen mit eigenen Verschlüsselungs- und Authentifizierungs-Lösungen vorab an den Markt. Leider sind hierfür vielfach neue Hardware-Telefone mit neuen Chipsätzen erforderlich, die bisher eingesetzten IP-Handapparate lassen sich nicht mit Verschlüsselung aufrüsten. Ähnlich wie für TK-Server vermarktet Cisco auch für die Telefone den Cisco Security Agent als Sicherheits-Software, über die erlaubte / unerlaubte Aktionen konfigurierbar werden und potenzielle Angriffe über ungewöhnliche Zugriffsmuster erkannt werden sollen.

Eine weitere Sicherheitsmaßnahme ist mittels Identifizierung über die Ethernet oder IP Adressen die Schaffung von separaten Voice VLANs für alle Telefone wie in Bild 3 gezeigt. Dieses Konzept funktioniert bei Hardware Telefonen, macht aber Schwierigkeiten bei Softphones, da diese nicht anhand ihrer Ethernet oder IP Adresse als Telefon erkennbar sind. Da Telefon-Sessions nicht über feste Portnummern laufen, ist derzeit auch kein generisches Prinzip möglich, ein Voice VLAN auf Softphones auszudehnen. Die Betriebskomplexität wird durch Voice VLAN's erhöht, da alle Etagenswitches, an denen Telefone und PC's angeschlossen sind, dann mit Tagging am Uplink konfiguriert werden müssen.

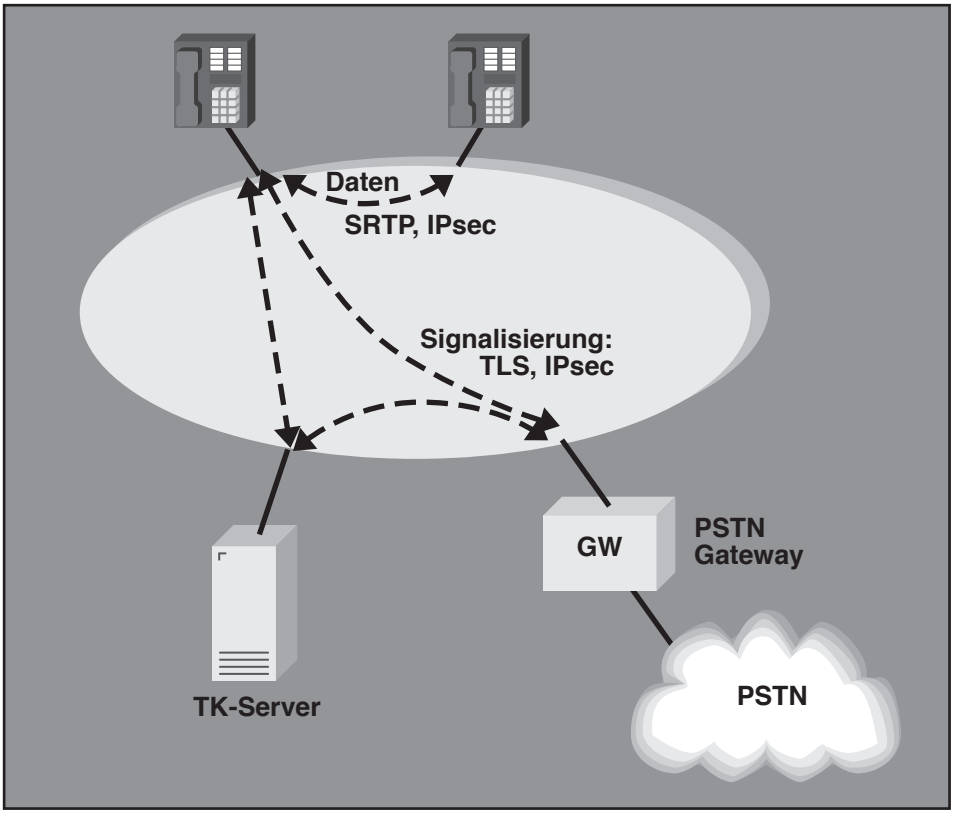
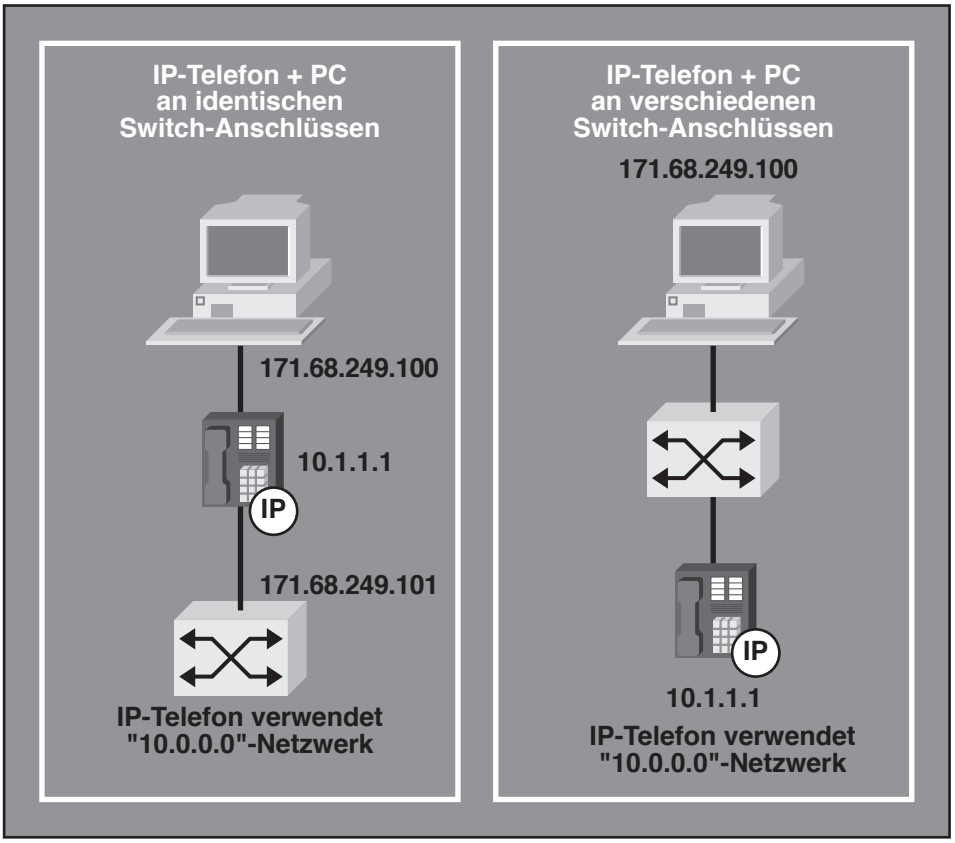


Bild 2: Verschlüsselung der Telefoniedaten am Endgerät

Bild 3: Konfiguration separater Voice VLANs



Voice-over-IP Lösungen und Sicherheit

VoIP Netzwerk

Zum Schutz gegen Angriffe können eine Reihe von Maßnahmen bei und mit den aktiven Netzwerkkomponenten durchgeführt werden:

Eine Kombination von Firewalls und Routern als Paketfilter bildet die Frontlinie gegen Angreifer. Sie müssen regelmäßig gegen neu bekannt gewordene ebenso wie gegen länger bekannte Angriffe getestet werden, um Verwundbarkeiten und Konfigurationsfehler aufzudecken.

Intrusion Detection und soweit sinnvoll Intrusion Prevention Systeme (IDS, IPS) können exponierte Netzwerkkomponenten zusätzlich absichern.

Logdateien müssen hinsichtlich unbefugter Zugriffe sowohl von Administratoren als auch Benutzern ausgewertet werden.

Authentifizierung der Benutzer kann z.B. bei Einwahl-Lösungen über RADIUS und im LAN über IEEE 802.1X (Port Security Standard für LAN Switches) realisiert werden.

Dateien für Konfigurations-Backup sollten verschlüsselt übertragen werden.

Werden Konfigurations-Dateien als Download mittels TFTP zu TK-Komponenten übertragen, so sollte dies über einen gut gesicherten Netzwerkpfad geschehen, ggf. mittels Tunneling / VPN.

Fazit: Die Entwicklungen gehen in die richtige Richtung

- Neue Versionen der TK Serversoftware sowie IP-Telefone unterstützen zunehmend notwendige Sicherheitsfunktionen.
- Für Server sind dies Authentifizierung und Verschlüsselung des Management-Zugriffs, Deaktivierung nicht benötigter Dienste und Systemfunktionen sowie Logeinträge.
- Für TK-Endgeräte sind dies Authentifizierung und Verschlüsselung des Datenanteils (Payload).
- Für den sicheren Betrieb einer VoIP Lösung sind entsprechende Schutzfunktionen im Netzwerk erforderlich wie Firewall, TK-DMZ, IDS / IPS. Diese sind jedoch in einer Reihe von Netzen ebenso für den sicheren Betrieb der bereits vorhandenen Serverfarm mit non-TK Applikationen notwendig.

Abkürzungen

ALG	Application Layer (Level) Gateway
CSA	Cisco Security Agent
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOS	Denial of Service
DDOS	Distributed DOS
EAP	Extensible Authentication Protocol
ENUM	E.164 Number and DNS (RFC 2916)
FW	Firewall
GW	Gateway
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over TLS/SSL
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOS	Internetworking Operating System (Cisco)
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
NAT	Network Address Translation
NFS	Network File System
PBX	Private Branch eXchange
PDA	Personal Digital Assistant
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial In User Service
RAS	Registration, Admission, Status
RCP	Remote Copy Protocol
RIP	Routing Information Protocol
RSH	Remote SHell Protocoll
RTCP	Real Time Control Protocol
RTP	Real-Time Protocol
SCP	Secure Copy
SIP	Session Initiation Protocol
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SRTP	Secure RTP
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TK	Telekommunikation
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless LAN

Neuer Kongress

Verkabelungs- und Infrastruktur-Forum 2004

Vom 3. bis 4. Mai veranstaltet die ComConsult Akademie im Hilton Hotel in Bonn das Verkabelungs- und Infrastruktur- Forum 2004.

Viele bestehende Verkabelungen für Lokale Netzwerke sind mittlerweile in die Jahre gekommen. Die zunehmende Integration von Gigabit-Teilnehmern, die Konzentration von Speichern und Servern im Rechenzentrum, aber auch die Umsetzung von IP-Telefonie generieren neue Anforderungen. Parallel entstehen für Neubauten durch eine geeignete Kombination aus Kabel und Funk völlig neue Lösungsansätze mit erheblichem Einsparpotenzial.

Das ComConsult Verkabelungs- und Infrastrukturforum 2004 analysiert die Technologie-, Markt- und Produktsituation und gibt wesentliche Empfehlungen sowohl zur Aktualisierung bestehender als auch zur Umsetzung neuer Infrastrukturen.

Im Einzelnen geht das Forum auf folgende Fragen ein:

- Welche Anforderungen müssen Verkabelungslösungen erfüllen, um den Herausforderungen der nächsten Jahre gewachsen zu sein?

Moderation:
Dipl.-Ing. Hartmut Kell

- Was ist der aktuelle Stand der Verkabelungs-Normierung? Welche speziellen Entwicklungen im Bereich EMV sind in Europa zu beachten?
- Sind Wireless-Netzwerke eine Alternative sowohl im Ausbau bestehender Kabelsysteme als auch als Komplettersatz in der Tertiärverkabelung?
- Wie sind bestehende Kabelsysteme zu bewerten? Welche Alternativen zur möglichst kostengünstigen Sanierung gibt es?
- Welche neuen Standards im Bereich Industrieverkabelung gibt es? Welche Stecksysteme, welche Kabeltypen werden sich durchsetzen?
- Was ist bei der Einhaltung von Brandschutzvorschriften zu beachten?
- Welche neuen Entwicklungen gibt es in der Messtechnik für Kupfer und LWL?
- In welchen Einsatzfällen ist Fiber-to-the-desk nach wie vor ein Thema, wie wird es umgesetzt?
- Sind optische Richtfunkstrecken im Gelände eine sinnvolle Option zur Senkung von Verlegekosten? Wo liegen Vor- und Nachteile?

Dieses Forum bietet die ideale Basis für eine Standortbestimmung. Wer immer eine Sanierung oder ein Redesign plant, wer nach sinnvollen Alternativen und Empfehlungen für optimale Lösungen sucht, der sollte dieses Forum nicht verpassen.

10 % Frühbucherrabatt bis 31.03.04

Verkabelungs- und Infrastruktur-Forum 2004

10.05. - 13.05.04 in Königswinter

Fax-Antwort an ComConsult 02408/955-399

Kongress-Anmeldung

☐ Ich melde mich an für das
ComConsult Verkabelungs- und Infrastruktur-Forum 2004
vom 03.05. - 04.05.04
zum Preis von € 1.340,-- zzgl. MwSt.*
(statt regulär € 1490,-- zzgl. MwSt.)

*Frühbucherpreis gültig bis 31.03.04

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

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Neue Zertifizierung

ComConsult Certified Security Ihr roter Faden zur IT-Sicherheit

Sicherheit, lange Zeit ein ungeliebtes Stiefkind, hat sich zu einem der wichtigsten Erfolgsfaktoren für den Einsatz von IT gemausert – für privatwirtschaftliche Unternehmen genauso wie für öffentliche Einrichtungen und Behörden.

Zum Teil zwingen gesetzliche Grundlagen zu einer bestimmten Qualität. Zum Teil entsteht der Zwang durch Wettbewerb: Vertrauen von Partnern und Kunden ist ein Wettbewerbskriterium! Wer sich eine Sicherheitspanne leistet oder erfolgreich aus dem Internet attackiert wird, ist in den Medien unangenehm präsent – und nichts ist schwerer wieder loszuwerden als ein einmal erworbener schlechter Ruf.

Alles in allem: IT-Sicherheit gewinnt stetig an Bedeutung.

Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Handbuchform beschriebene IT-Grundschutz stellt dabei eine anerkannte und tragfähige Basis dar. Wer hierauf aufsetzt, schafft eine gute Grundlage, ob nur zum eigenen Schutz oder auch zur Dokumentation der eigenen Sicherheitsqualität über die angebotene BSI-Zertifizierung. Wer konsequent nach BSI-Grundschutzhandbuch vorgeht, verhält sich zugleich konform zum im internationalen Bereich stärker diskutierten Sicherheitsstandard BS7799.

Aber Vorsicht: Ein Handbuch ist so nützlich wie seine erfolgreiche Umsetzung in der Praxis – und hier liegen Erfolg und Desaster eng beieinander. Wer zu lange „ganzheitlich“ und „top down“ nachdenkt und konzipiert, ist lange schwach oder lückenhaft geschützt und nass, bevor der Schirm auf ist. Wer aber ausschließlich ohne Gesamtkonzept und Strategie sicherheitstechnische Einzelmaßnahmen schafft, erhält ein Flickwerk, kein schützendes „Haus der Sicherheit“ mit allen notwendige Standbeinen: Technik, geeignete Prozesse zum Betrieb dieser Technik und sicherheitsbewusste Nutzung der IT. Und dann sollen womöglich noch Vorschriften für ein Zertifizierungsverfahren berücksichtigt werden?!

IT-Sicherheits-Experten der ComConsult Beratung und Planung GmbH haben genau dieses Dilemma in etlichen Kundenprojekten angetroffen und bewältigt.

Aufbauend diesen Erfahrungen wurde in Zusammenarbeit mit Dr. Jürgen Suppan

die ComConsult Certified Security (kurz: C³Sec) als Vorgehensweise etabliert. C³Sec verfolgt den Ansatz, zunächst die wesentlichen Kernbereiche effektiv abzusichern, ohne durch diesen Sofortschutz den Weg zu einer IT-Sicherheitsinfrastruktur mit zertifizierbarer Qualität unnötig aufwändig werden zu lassen.

Genau diese Kombination aus Pragmatismus, Orientierung am Gesamtziel in jedem Schritt und Berücksichtigung des BSI-Grundschutzes als anerkanntem und zertifizierbarem Standard ist das Besondere von C3Sec. Das ist effizienter und wirksamer Umgang mit dem Thema Sicherheit: keine Blindleistung durch Aktionismus, keine eklatanten Sicherheitslücken in der Startphase, kein Nachbessern an Schritten der ersten Stunde für eine mögliche abschließende Zertifizierung.

Und so funktioniert C³Sec:

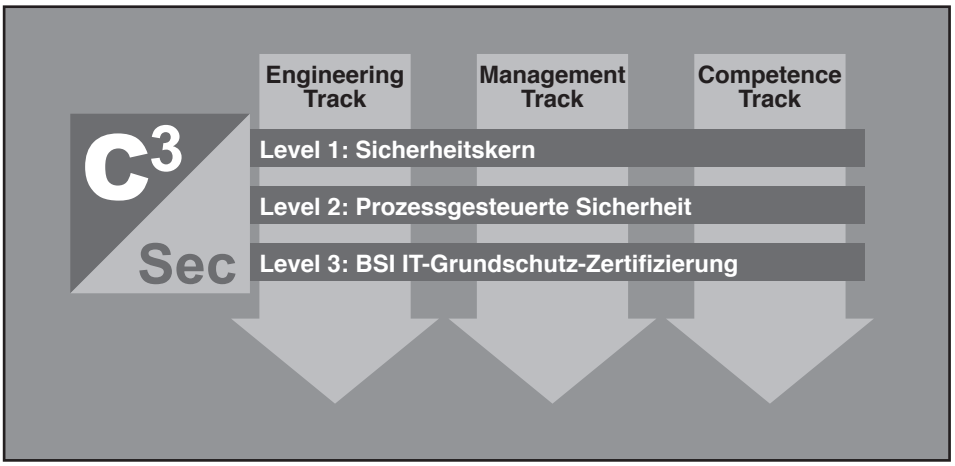
Unter geeigneter Berücksichtigung dreier sich notwendig ergänzender Pfade auf dem Weg zur angemessenen und mit Zertifikat belegbaren IT-Sicherheit wird die Qualität der IT-Sicherheit einer Kundenumgebung in gezielten Schritten von Level zu Level angehoben (Bild 1).

Die drei parallel beschrittenen Pfade bilden zusammen die Grundlage eines gelebten IT-Sicherheitsprozesses. Der Engineering Track umfasst technische Konzipierung, Umsetzung und Betrieb von Sicherheitsmaßnahmen. Der Management Track beinhaltet die Ermittlung des konkreten, umgebungsspezifischen Schutzbedarfs der einzelnen Geschäftsprozesse, die Risikoanalyse und Kosten-Nutzen-Betrachtung zu IT-Sicherheitsmaßnahmen. Im Competence Track wird schließlich gezielt der „Risikofaktor“ Mensch betrachtet – durch Sicherstellung des notwendigen Sicherheits-Know-how der Administratoren, Vermittlung der Notwendigkeit von IT-Sicherheitsmaßnahmen an die IT-Nutzer und Unterweisung in dementsprechendem Umgang mit der IT.

Erst die Kombination dieser Ansatzpunkte gewährleistet eine tragfähige IT-Sicherheit.

Der zuerst erarbeitete Level 1 („Sicherheitskern“) konzentriert sich dabei auf die als besonders kritisch identifizierten Sicherheitssysteme, mindestens die Bausteine Firewall-System, Virenschutz, Datensicherung, Zugangsschutz / Infrastruktursicherheit und IT-Sicherheitsmanagement.

Bild 1: C³Sec-Strategie: Schrittweise Erhöhung der Sicherheitslevels



ComConsult Certified Security

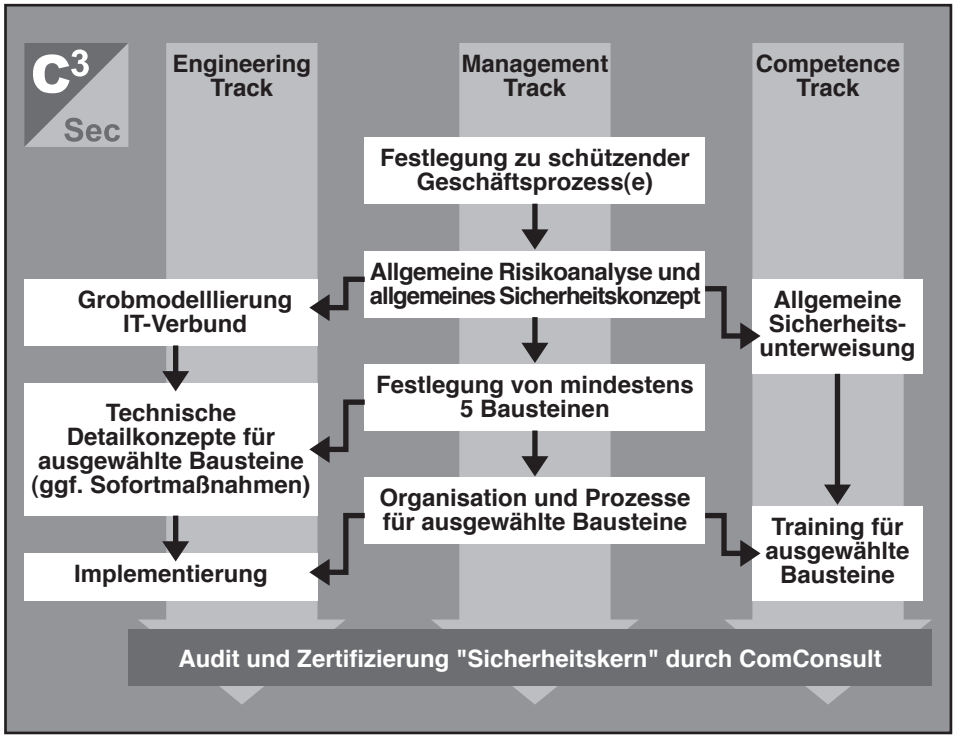


Bild 2: Audit und Zertifizierung "Sicherheitskern" durch ComConsult

Für diese wird sofort eine angemessene Implementierung konzipiert und umgesetzt sowie ein geordneter Betrieb etabliert (Bild 2)

Wegen der Beschränkung auf die besonders kritischen Grundsysteme und -prozesse wird im Level 1 noch kein geschlossenes IT-Sicherheitskonzept gemäß BSI-Grundschutzhandbuch erreicht. Die Level-1-Zertifizierung durch ComConsult bestätigt aber bereits, dass die wesentlichen Sicherheitssysteme des Unternehmens geordnet und BSI-konform betrieben werden. Damit ist auch der Grundstein für eine spätere BSI-Zertifizierung gelegt. Im Rahmen der Ist-Aufnahme kommt hier der Fragebogen aus der neuen BSI-Veröffentlichung IT-Grundschutzkompakt zur Anwendung.

Level 2 fügt der so geschaffenen grundlegenden Sicherheit die notwendige Geschlossenheit und Prozess-Orientierung hinzu („prozessgesteuerte Sicherheit“),

Jetzt wird eine umfassende IT-Sicherheitsstrategie festgelegt, auf deren Basis schrittweise der Sicherheitskern erweitert werden kann. Jetzt tritt bewusst der Sicherheitsprozess an die Stelle punktueller Einzeloptimierungen, und für die effiziente, kontinuierliche Anpassung an sich ändernde Anforderungen und Rahmenbedingungen wird durch Integration der Ergebnisse in die allgemeinen IT-Prozesse der Boden bereitet (Bild 3).

In dieser Stufe kann bereits eine Selbsterklärung beim BSI abgegeben und so eine erste Außenwirkung der bisherigen Maßnahmen erreicht werden.

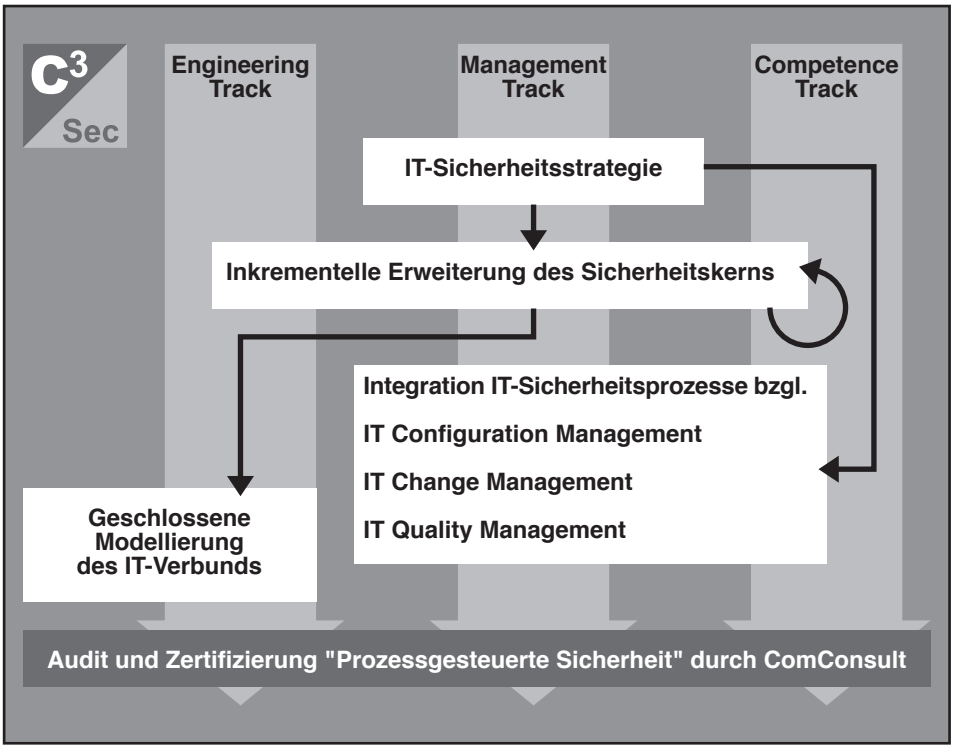
Für eine als Level 3 zu erreichende IT-Grundschutzzertifizierung sind abschließend die Formalien des vorgeschriebenen Zertifizierungsverfahrens zu durchlaufen, die eine Überprüfung von IT-Strukturanalyse, Schutzbedarfsfeststellung, Modellierung des „IT-Verbundes“ und IT-Grundschutzerhebung umfassen.

Diese Überprüfung wird anhand des vom BSI vorgeschriebenen Prüfschemas für Auditoren vorgenommen.

Da durch die ComConsult-Berater bei den Arbeiten zur Erreichung der C³Sec-Level 1 und 2 bereits auf eine zertifizierungstaugliche Dokumentation geachtet wird, muss hier nicht mühsam nachgebessert werden! Vielmehr ist im wesentlichen das vorgeschriebene Prüfverfahren mit Hilfe eines unabhängigen, autorisierten BSI-Grundschutz-Auditors als formaler Akt zu durchlaufen.

Sind alle Überprüfungen erfolgreich abgeschlossen, erfolgt die (Anmeldung zur) Grundschutzzertifizierung beim BSI.

Bild 3: Audit und Zertifizierung "Prozessgesteuerte Sicherheit" durch ComConsult



CCSE

1. ComConsult Certified Security Expert

Bernd Reklies (48), Diplom-Informatiker, arbeitet bei den Howaldtswerken Deutsche Werft AG in Kiel seit 17 Jahren, speziell im IT-Security-Bereich seit 4 bis 5 Jahren. Ursprünglich kam er aus der UNIX-Administration und konfigurierte z.B. Solaris-Maschinen. Der Netzwerk Insider sprach mit ihm unmittelbar nach seiner bestandenen Prüfung zum "ComConsult Certified Security Expert".

Insider: Erzählen Sie uns bitte etwas über Ihr Arbeitsfeld.

Bernd Reklies: Meine Aufgaben jetzt sind es z.B. Firewall-Systeme zu administrieren, neue Security-Konzepte wie Notebook-Security und WLAN-Verbindung zu konzipieren, auszuarbeiten und dann entsprechende Entscheidungen auszuarbeiten. Wir sind im Team 3 - 4 Kollegen, aber dies sind schwerpunktmäßig meine Aufgaben.

Insider: Wie kamen Sie dazu „ComConsult Certified Security Expert“ zu werden?

Bernd Reklies: Ich habe schon einige Sicherheits-Kurse bei ComConsult gemacht und mehrmals das Security-Forum besucht. Ich bin ein Mann der Praxis und habe in dieser Ausbildung die Möglichkeit gesucht, meine Fähigkeiten und den Wissensstand, den ich selbst habe, einfach mal zu überprüfen. Ich habe mit dem CCSE erstmals eine Prüfung gefunden, die hersteller- und produktneutral mein Wissen im Rahmen der IT-Security testet. Ich wollte für mich selbst herausfinden, ob ich überhaupt genug weiß aus dem Bereich der Security. Ich habe dann festgestellt, dass ich aufgrund der Unterlagen und der praktischen Arbeiten während der Kurse eine ganze Menge in der Praxis umsetzen konnte. Durch das Aufbereiten der Themen und die Vorbereitung auf die Prüfung wurde ich in die Lage versetzt, auf aktuelle Projekte Einfluss nehmen zu können.

Insider: Wie haben Sie sich auf die Prüfung vorbereitet?

Bernd Reklies: Die Vorbereitung auf die Prüfung war aus meiner Sicht recht schwierig. Die Prüfungsfragen sind sehr umfangreich, die Aufgabenstellungen waren oft nicht leicht zu beantworten. Häufig war es auch so, dass man sich erst noch mal schlau machen musste, um eine passende Antwort zu finden, d.h. man musste im Internet recherchieren oder mit Kollegen über das Thema diskutieren.

Mit dem ComConsult Certified Security Expert (CCSE) bietet die ComConsult Akademie eine systematische Ausbildung zum/r Sicherheits-Spezialisten/in für Netzwerk- und IT-Technologien an. Die Ausbildung ist so aufgebaut, dass alle wesentlichen Technologien vom Netzwerk bis zur Clienten-Sicherheit im Sinne des stufenweisen Aufbaus einer Gesamtlösung abgedeckt werden.

Die Ausbildung basiert auf drei Intensiv-Kursen "Sicherheitslösungen", davon zwei 5-tägig und einer 3-tägig.

- Kurs 1: "Von den Einzelbausteinen zur integrierten technischen Lösung"
- Kurs 2: "IP-VPNs, der Kern einer Sicherheits-Infrastruktur"
- Kurs 3: "Planung und praktische Konfiguration"

Die Ausbildung endet mit der Prüfung zum CCSE, die aus einer Mischung aus schriftlicher und mündlicher Prüfung besteht.

Insider: Wie sind die Kurse für Sie gelaufen?

Reklies: Das erste Seminar der Ausbildung „Sicherheits-Lösungen I: Von den Einzelbausteinen zur integrierten Lösung“ habe ich im Juni letzten Jahres gemacht. Zu diesem Zeitpunkt wollte ich einfach nur den Grundlagenkurs besuchen, habe dann aber im Dezember auch die beiden weiterführenden Kurse belegt und zu diesem Zeitpunkt auch den Entschluss gefasst, die Zertifizierung zu machen. Die Abschlussprüfung habe ich auf privater Basis gemacht, denn mein Arbeitsgeber meinte, ich wüsste schon alles, das bräuchte ich doch gar nicht und ihm würde meine Zertifizierung eigentlich nichts nutzen. Ich wollte aber – wie gesagt – für mich selbst meinen Wissensstand überprüfen.

Insider: Sie kommen gerade aus der Prüfung. Haben Sie sich das so vorgestellt?

Bernd Reklies: Herr Meder hat die Prüfung äußerst korrekt vorgenommen. Er ist da sehr genau und man hat das Gefühl, man bekommt nichts geschenkt. Das habe ich als sehr positiv empfunden, denn das gibt dem Zertifikat auch seine Wertigkeit.

Insider: Und was machen Sie jetzt mit dem Zertifikat?

Bernd Reklies: Ich weiß es noch nicht, vielleicht fotokopieren und an die Wand hängen. Ich werde es jetzt erst mal zu meinen Unterlagen packen. Es findet sich bestimmt ein Anlass, wo ich es gebrauchen kann.

Insider: Planen Sie weitere Kursbesuche bei ComConsult?

Bernd Reklies: In unserer Branche ist man gezwungen, sich ständig fortzubilden. Ich werde auf jeden Fall versuchen, beim IT-Security Kongress* von ComConsult im Mai dabei zu sein. Ich verspreche mir davon einen regen Informationsaustausch mit den Kollegen und erwarte einen Überblick über die neuesten IT-Sicherheitsfragen.

Insider: Vielen Dank für das Interview und viel Erfolg für Ihre weitere berufliche Zukunft.

* ComConsult IT-Sicherheitsforum 2004, siehe Seite 4

Schwerpunktthema

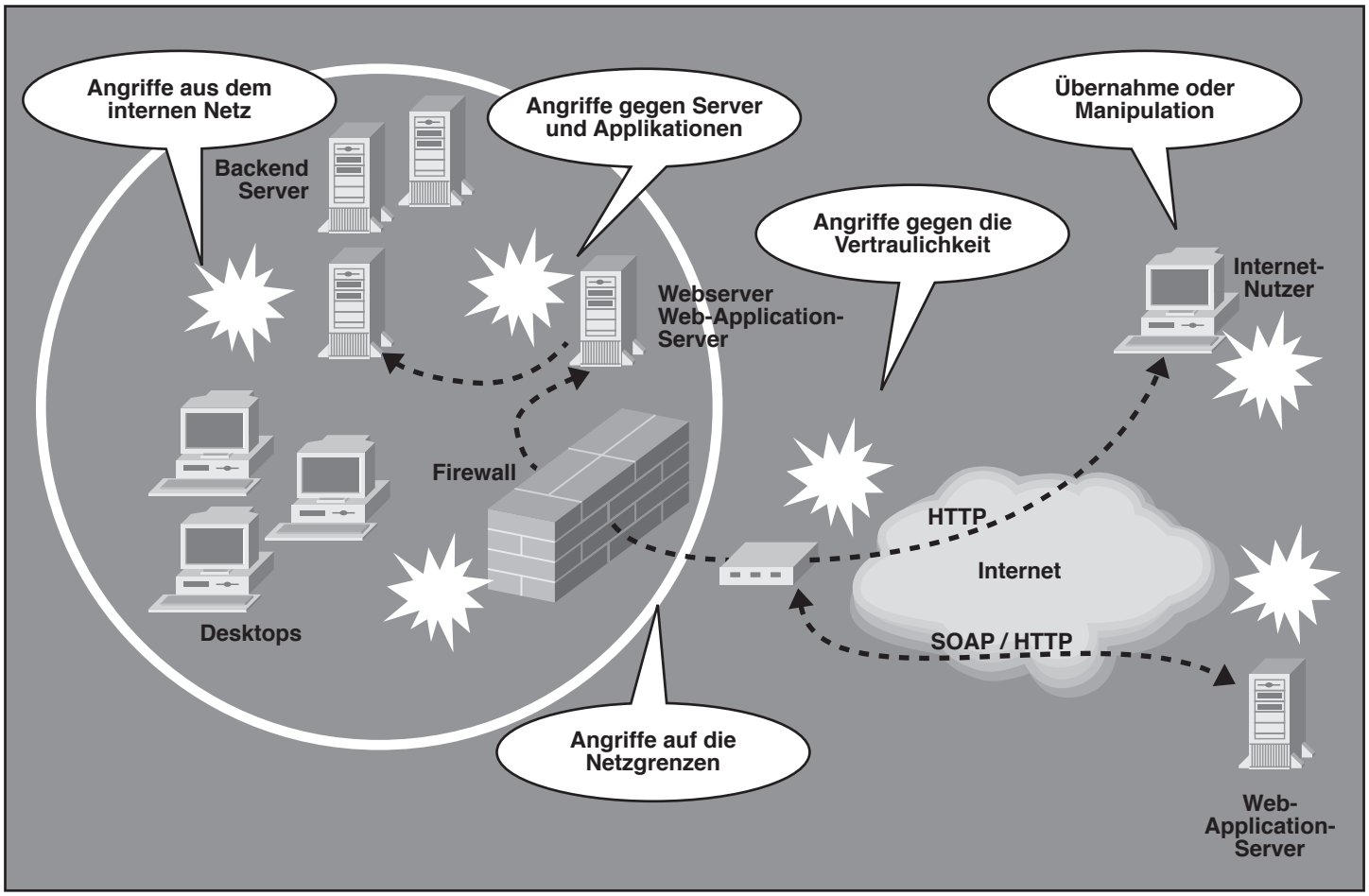
Web-anwendungen: Die neue Hintertür ins Unternehmen?

Fortsetzung von Seite 1

Dipl.-Inform. Detlef Weidenhammer ist als Geschäftsführer der GAI NetConsult GmbH vorwiegend auf den Gebieten Internet/Intranet-Anwendungen und Netzwerk-Sicherheit tätig. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen als Fachberater und auch als Referent bei Seminaren und Kongressen ein.

Dem Thema Sicherheit ist bei der Erstellung und Nutzung von Webanwendungen eine besondere Bedeutung beizumessen. Dies ist für die Nutzerakzeptanz immens wichtig, ebenso aber auch für den Anbieter selber, der für die bereit gestellten Ressourcen Verantwortung trägt. Für den Nutzer ist der Schutz seiner persönlichen Daten und der Transaktionsdaten während der Übertragung von großer Bedeutung. Für den Anbieter ergeben sich ganz neue Risiken, wenn die Webanwendung komplexe Funktionen mit Zugriff auf interne Datenbestände bereitstellt. Damit hat prinzipiell jeder Teilnehmer im Internet die Möglichkeit mittels einfacher HTTP-Requests die Sicherheit dieser Anwendung zu testen. Angriffsversuche verbergen sich im legitimen HTTP-Datenstrom und werden durch keine Firewalls oder Intrusion-Detection Systeme erkannt und auch nicht durch den Einsatz einer SSL-Verschlüsselung verhindert. Es ergeben sich damit eine Vielzahl von Sicherheitsproblemen bei Webanwendungen (siehe Bild 1).

Bild1: Sicherheitsprobleme bei Webanwendungen



Webanwendungen: Die neue Hintertür ins Unternehmen?

Als wesentlicher Punkt ist festzuhalten: die Webanwendung ist Teil der Netzgrenze des Unternehmens (des Perimeters) und damit ebenso gut wie diese zu schützen.

Doch wie sieht die Realität aus? Herkömmliche Schutzmaßnahmen mit Firewalls haben ihre Stärken in der Kontrolle auf Netzebene, können aber auf Anwendungsebene bestenfalls offensichtlichen Missbrauch erkennen.

Aktuelle Angriffe zielen aber eher auf Schwachstellen innerhalb einer Anwendung. Ursache hierfür ist zumeist die mangelhafte Beachtung von Sicherheitsaspekten bei der Program-mierung. Besonders attraktiv für Angreifer ist die Tatsache, dass für einen Großteil der möglichen Attacken kein spezielles Tool benötigt wird, ein Standard-Webbrowser ist vollkommen ausreichend. Manipulierte HTTP-Requests sind somit in der Lage, Schwachstellen auf allen Ebenen einer Webanwendung auszunutzen (siehe Bild 2).

Wie deshalb auch zu erwarten war, konnte man in der letzten Zeit eine deutliche Zunahme der Angriffe auf Webanwendungen registrieren. Die alljährliche Studie von CSI/FBI (www.gocsi.com) ermittelte 2003 bei insgesamt 53% der befragten Unternehmen Angriffe auf deren Websites. Die Gartner Group berichtete in einem Bericht (03/2003) über eine Erfolgsquote von 75% bei Tests von Webanwendungen. Diese erschreckenden Ergebnisse decken sich mit unseren eigenen Erfahrungen aus einer Vielzahl von Sicherheitsüberprüfungen. Dabei konnten wir sogar bei über 90% der untersuchten Webanwendungen die gefundenen Schwachstellen zu gravierenden Manipulationen ausnutzen.

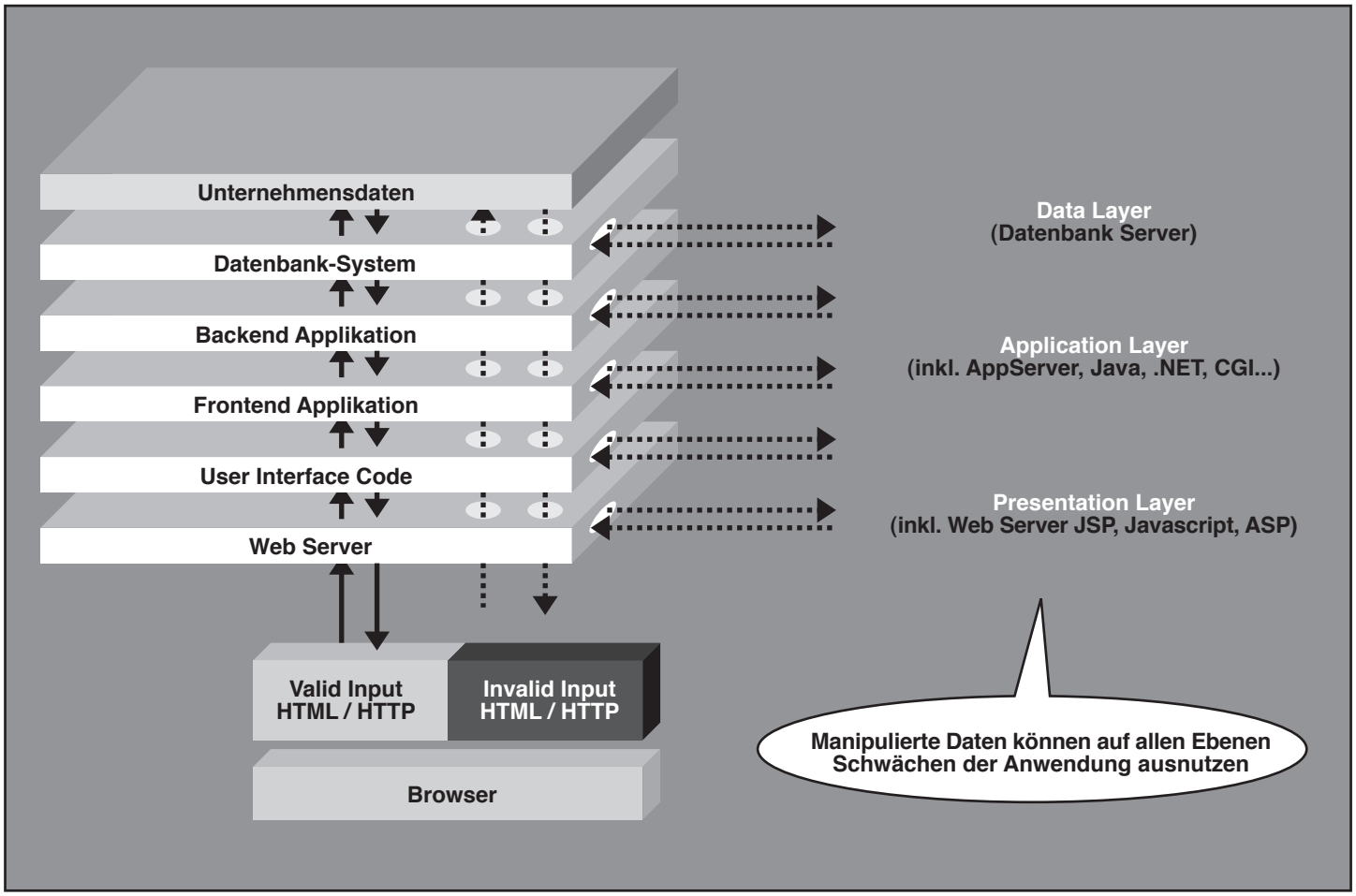
Hierzu gehörten:

- Ausführen von Kommandos auf dem Webserver oder auf fremden Clients
- Vollständige Übernahme des Webservers
- Eindringen in das Unternehmensnetz
- Verändern der Webdarstellung („defacement“)
- Übernahme von fremden Sessions
- Auslesen von (intern gehaltenen) Datenbank-Inhalten

Welche Haltung die Hersteller zum Thema Sicherheit bei Webanwendungen einnehmen, lässt sich am ehesten mit einer Aussage von Microsoft zu Web-Services belegen: "Since SOAP relies on HTTP as the transport mechanism, and most firewalls allow HTTP to pass through, you'll have no problem invoking SOAP endpoints from either side of a firewall”.

Diese schon länger als „Port-80 Problematik“ bekannte Unsitte, den bei den meisten Unternehmen erlaubten HTTP-Verkehr zum Durchtunneln von Firewalls auch für andere Dienste zu nutzen, wird uns also wohl noch längere Zeit begleiten. Grund genug, sich mit den wichtigsten Bedrohungen bei der Nutzung von Webanwendungen intensiv zu beschäftigen.

Bild 2: Zielpunkte manipulierter HTTP-Requests



Webanwendungen: Die neue Hintertür ins Unternehmen?

Typische Sicherheitslücken in Webanwendungen

Nachfolgend werden die am häufigsten anzutreffenden Fehler bei der Implementierung einer Webanwendung und die daraus resultierenden Sicherheitslücken und Bedrohungen aufgezeigt und Möglichkeiten angegeben, wie diese vermieden werden können.

Die Liste basiert auf der aktuellen Veröffentlichung des OWASP-Projekts – Open Web Application Security Project (www.owasp.org), „The Ten Most Critical Web Application Security Vulnerabilities – 2004 Update“) und unseren eigenen Erfahrungen aus Sicherheitsüberprüfungen von Webanwendungen.

B1: Nicht validierte Eingabeparameter

Diese sind für den Großteil aller erfolgreichen Angriffe auf Webanwendungen verantwortlich. Es sollte nie vergessen werden: Alle Parameter einer HTTP-Anfrage sind manipulierbar. Dazu gehören beispielsweise die URL, sämtliche HTTP-Header, Cookies und Formularfelder. Einige besonders erwähnenswerte Angriffsformen wie SQL-Injection oder Buffer Overflows werden später gesondert angesprochen. Betroffen sind alle Webanwendungen, unabhängig von Serverversionen oder Programmiersprachen. Bei der Validierung der übergebenen Parameter ist darauf zu achten, dass diese serverseitig erfolgt. Eine clientseitige Überprüfung der Parameter ist nicht sinnvoll, da ein Angreifer diese leicht umgehen kann. Grundsätzlich sollte nie davon ausgegangen werden, dass ein Angreifer sich so verhält, wie es in der Anwendung vorgesehen ist. Eine Vielzahl von Angriffen wäre nahezu unmöglich, wenn Entwickler die Validierung von Parametern wirklich Ernst nehmen würden.

Maßnahmen: Alle durch den Anwender übergebenen Parameter sind vor der Verarbeitung innerhalb der Anwendung zu validieren. Es bietet sich an, diese Validierung in eine zentrale Funktion oder Bibliothek auszulagern, um eine saubere Code-Struktur zu erreichen oder zu erhalten. Grundsätzlich ist bei der Überprüfung der Eingaben der Einsatz von Positivlisten zu empfehlen.

Minimal sollten folgende Parameter gegen eine Positivliste validiert werden:

- Eingabetyp (String, Integer usw.)
- Erlaubte Zeichen (nur Zahlen, nur Buchstaben usw.)
- Minimale und maximale Länge
- Wertebereich
- Spezifische Pattern und erlaubte Werte

In den letzten Monaten ist eine Vielzahl von Produkten aufgetaucht, die vorgeben, genau diese Validierung vornehmen zu können, einige davon werden später kurz vorgestellt. Grundsätzlich ist es aber sinnvoller, die benötigten Funktionen in die Anwendung selbst einzubauen.

B2: Ungenügende Zugriffskontrolle

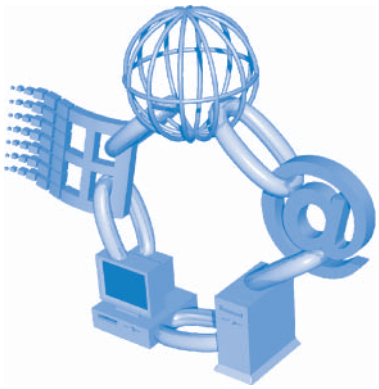
Zugriffskontrollen (Autorisierungen) in einer Anwendung legen fest, auf welche Funktionen und Inhalte Anwender zugreifen dürfen. Diese Kontrollen werden nach erfolgreicher Authentisierung durchgeführt. Viele Anwendungen klassifizieren Anwender anhand bestimmter Rollenprofile. Ein Angriffsszenario wäre daher, dass sich ein nur mit geringen Privilegien ausgestatteter Nutzer Zugriff auf die Daten eines höher privilegierten Nutzers verschafft und so im schlimmsten Fall die Kontrolle über die Anwendung übernehmen kann. Ermöglicht wird dies zumeist durch fehlende Planung der Zugriffsregeln und unsaubere Programmierung (Zeitdruck!), die die Komplexität dieser wichtigen Sicherheitsfunktion total unterschätzt.

Besonders zu beachten sind administrative Zugriffe über das Internet auf die Anwendung, zumeist genutzt für das Management von Anwendern, Daten und Inhalten. Diese Zugänge sind ein beliebtes Ziel für Angreifer, da hier die Möglichkeit lockt, sich mit einem Schlag administrative Privilegien innerhalb der Anwendung zu verschaffen.

Häufig auftretende Probleme sind:

- Fehlende Separierung von Anwender- und Administratorzugang
- Schwache Authentisierung der administrativen Nutzer
- Unverschlüsselte Kommunikation bei Nutzung der administrativen Zugänge

Seminar zum Thema



Sicherheits-Lösungen: Von den Einzelbausteinen zur Integrierten Lösung

Seminar

01.03. - 05.03.04 Köln
03.05. - 05.05.04 Zürich
24.05. - 28.05.04 Köln

Dieses Seminar vermittelt, aus welchen Bausteinen eine effiziente Sicherheits-Lösung aufgebaut wird, welche Bausteine unverzichtbar sind und wie diese Bausteine konfiguriert werden. Jeder einzelne Baustein wird detailliert erklärt und in seinen Potenzialen beschrieben. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.
Referenten: Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hans-Peter Mohn,
Einzelpreis: € 2.290,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Webanwendungen: Die neue Hintertür ins Unternehmen?

Maßnahmen: Es ist dringend zu empfehlen, eine Matrix über alle Zugriffsregeln aufzustellen, die kontrollierbar festlegt, welche Nutzer auf bestimmte Systeme und Daten zugreifen dürfen. Die korrekte Umsetzung innerhalb der Anwendung ist ausgiebig zu testen.

Besonders zu beachten sind:

• Sichere Vergabe von IDs

Die meisten Webanwendungen nutzen auf sehr unterschiedliche Art generierte IDs zur Referenzierung von Anwendern, Rollen, Inhalten, Objekten oder Funktionen. Kann ein Angreifer das Vergabeschema ermitteln und versagt bei Zugriffen der Abgleich mit den aktuellen Rechten dieses Anwenders, ist er in der Lage die Zugriffskontrolle zu testen oder sogar zu umgehen.

• Umgehen der Zugriffskontrolle durch direkten Zugriff auf Webseiten

Die Anwendung darf es nicht zulassen, dass ein Angreifer direkt auf bestimmte Webseiten zugreift und so den Authentisierungsvorgang übergeht. Auch hier muss die Validierung serverseitig erfolgen, die Auswertung von clientseitigen Parametern, wie beispielsweise der "Referer Header-Zeile" können durch einen Angreifer leicht umgangen werden.

• Direkte Dateizugriffe

Auch bei Einsatz eines Datenbank-Backend-Servers liegen häufig einzelne Dateien wie Konfigurationsvorlagen in einem für den Anwender zugänglichen Bereich des Web- oder Applikationsservers. Hier muss über restriktive Dateizugriffsberechtigungen verhindert werden, dass ein Angreifer diese öffnen kann.

Grundsätzlich sollte eine Fernadministration "durch die Vordertür", also über den gleichen Weg, den auch die Anwender nutzen, vermieden werden. Bessere Methoden sind aus Sicherheitssicht die Nutzung eines VPNs oder einer stark authentisierten RAS-Einwahl in das LAN mit anschließender Nutzung der internen Administrationswege. Ist aber der administrative Zugang über Nutzer-Webschnittstelle zwingend erforderlich, sollte hier in jedem Fall eine Sicherung des Transportwegs mit SSL sowie eine starke Authentisierung über One-Time-Password Token oder Smart Card erfolgen. Komplexere Anwendungen sollten auch über administrative Rollen verfügen, um beispielsweise Nutzeradministration und die Verwaltung der Inhalte trennen zu können.

B3:
Ungenügende Authentisierung und Session Management

Authentisierung und Session Management behandeln alle Aspekte der sicheren Nutzer-Identifikation von Sitzungskontrolle. Aber selbst die besten Authentisierungsmethoden sind wenig wert, wenn das zugehörige Management fehlerhaft umgesetzt wurde. Zur Authentisierung bei Webanwendungen werden heute zumeist immer noch Userid und Passwort benutzt. Die weitaus besseren Methoden unter Nutzung von Hard- und Softtoken oder biometrischen Verfahren kommen in erster Linie aus Kostengründen nur selten zum Einsatz.

So gut wie alle Webanwendungen nutzen eine Form von Session ID zur Identifizierung eines Nutzers. Begründet ist dies vor allem in der Tatsache, dass das Transportprotokoll HTTP zustandslos ist, also selbst keine Möglichkeit zur Unterscheidung zweier Nutzer bietet. Session IDs werden meist in Form von Cookies oder über URL-Rewriting realisiert. Erfolgt die Vergabe der Session IDs nach einem vorhersagbaren Muster, so kann ein Angreifer sich Zugang zu den Daten eines anderen Anwenders verschaffen, ohne sich vorher authentisieren zu müssen. Wenn Authentisierungsinformationen und Session-IDs nicht mittels SSL geschützt werden, besteht immer die große Gefahr, dass es einem Angreifer gelingt, die Identität oder Sitzung eines anderen Anwenders zu übernehmen.

Maßnahmen: Aufbauend auf Vorgaben einer Security Policy sollte eine sorgfältige und angemessene Implementierung von Authentisierung und Session Management die Angriffsmöglichkeiten deutlich einschränken. Die korrekte Umsetzung innerhalb der Anwendung ist ausgiebig zu testen. Besonders zu beachten sind:

• Sichere Handhabung von Passwörtern

Passwörter sind noch immer die Authentisierungsmethode Nummer eins. Zur sicheren Handhabung dieser zählen beispielsweise die Erstausstellung eines Passworts und die Vermeidung des Klartextversands von Passwörtern (z. B. per E-Mail). Je nach Anforderungen an die Sicherheit der übermittelten Daten sollte das Erstpasswort beispielsweise per Postversand übermittelt werden. Bei fehlgeschlagenen Logins sollten die übermittelten Daten nicht dauerhaft gespeichert werden. Am Verhalten der Anwendung sollte sich nicht erkennen lassen, welche Komponente (Kennung oder Passwort) der Authentisierungsdaten fehlerhaft war.

Seminar zum Thema

Sicherheits-Lösungen: IP-VPNs, der Kern einer Sicherheits-Infrastruktur

Seminar

22.03. - 24.03.04 Bonn
28.06. - 30.06.04 Köln

Das Seminar beschäftigt sich mit den Nutzungsformen, den Realisierungs-Alternativen und der Integration in bestehende Netzwerk-Infrastrukturen von VPN-Technologie, wie z.B. die optimale Kombination eines VPN-Servers mit Firewall/Routing/NAT oder die Klärung der Microsoft-spezifischen Fragen auf den Client-PCs (Interoperabilität, Anmeldung, Namensauflösung)
Referenten: Dipl.-Inform. Andreas Meder, Alexander Zarenko
Einzelpreis: € 1.690,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

• Starke Passwörter

Je nach den Anforderungen an die Sicherheit der übertragenen Daten sind starke Passwörter (mindestens acht Zeichen, Buchstaben, Zahlen und Sonderzeichen) zu erzwingen. Diese sollten periodisch gewechselt werden, wobei die Wiederverwendung alter Passwörter zu verhindern ist.

• Speicherung der Passwörter

Passwörter sollten nach Möglichkeit nicht im Klartext, sondern nur in verschlüsselter oder gehashter Form abgelegt werden. Präferiert wird die Speicherung eines Hashes, da dieser nicht reversibel ist. Passwörter sollten nicht im Sourcecode der Anwendung gespeichert werden.

• Schutz bei der Übermittlung der Passwörter

Der einzig wirksame Schutz der Passwörter ist die Nutzung von SSL, da nur so Replayattacken vermieden werden können.

• Schutz der Session ID

Die Session ID ermöglicht der Anwendung, einen bereits authentisierten Nutzer von einem nicht authentisierten Nutzer zu unterscheiden. Die Anforderungen an den Schutz der Session ID entsprechen daher denen, die an den Schutz des Passwortes gestellt werden. Bei jeder Änderung des Zustands einer Sitzung, wie beispielsweise von unverschlüsselt auf SSL-gesichert, oder vor der Durchführung einer Transaktion ist eine neue Session ID zu generieren. Nutzerspezifizierte Session IDs sind zu verwerfen.

• HTTP-Methoden

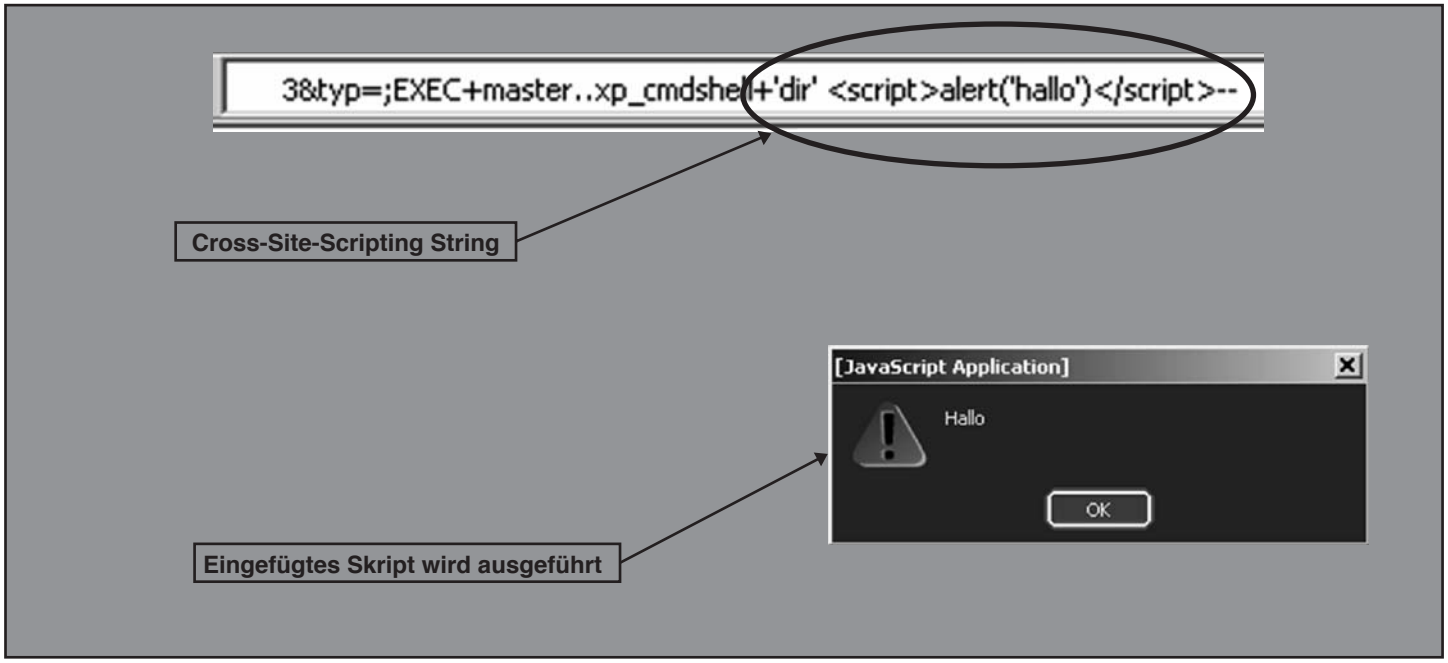
Authentisierungsdaten (Nutzerkennung und Session ID) sollten nie per HTTP GET übertragen werden, da diese Daten dann eventuell auf Proxies und im Browsercache des Klienten zwischengespeichert werden. Die Nutzung der HTTP-Methode POST verhindert dies. Zusätzlich sind bei Übermittlung von Authentisierungsdaten alle HTML-Varianten des “No Cache“-Tags anzuwenden.

B4:
Cross-Site Scripting (XSS)

Cross-Site Scripting ist immer dann möglich, wenn eine Anwendung die Eingaben eines Nutzers ungeprüft für die Erstellung einer neuen Webseite nutzt. Ein Angreifer kann so HTML oder Skript-Code im Kontext der Webseite zur Ausführung bringen. Anzumerken ist hier, dass das Ziel des Angriffs der Nutzer der Anwendung und nicht die Anwendung selbst ist. Unterschieden werden zwei Arten von Cross-Site Scripting: permanentes und dynamisches XSS. Permanente Angriffe sind möglich, wenn die durch den Angreifer eingegebenen Daten dauerhaft in der Anwendung gehalten werden. Besonders gefährdet sind hier Webforen, die ja darauf angewiesen sind, dass Anwender neue Daten eingeben können. Neben den permanenten XSS-Attacken gibt es auch die dynamische Form des Cross-Site Scriptings, hier ist der Angreifer darauf angewiesen, dass der Nutzer auf einen durch den Angreifer vorgegebenen Link klickt, der dann den Code des Angreifers zur Ausführung bringt. Klassisches Beispiel für dynamisches Cross-Site Scripting sind Fehlerseiten, die die Eingaben des Anwenders eins zu eins zurückgeben.

Die Konsequenzen eines XSS-Angriffs sind abhängig von der eingesetzten Anwendung. Im schlimmsten Fall kann ein erfolgreicher Angriff aber in der Kompromittierung eines Nutzerkontos resultieren, wenn es einem Angreifer gelingt, den Session Cookie des Nutzers in seinen Besitz zu bringen. Denkbar sind aber auch Angriffe auf Anwendungen, die nicht nutzerbezogen arbeiten. Man stelle sich zum Beispiel die Webseite einer Bank vor, auf deren Homepage ein gefälschter News-Beitrag wie dieser zu finden ist: „Gewinnwarnung der Telekom, wir raten zum sofortigen Verkauf der Aktien“. Dieser Beitrag wäre zwar nur für die Nutzer sichtbar, die der Angreifer dazu gebracht hat, auf den vom ihm vorgegebenen Link zu klicken, was aber wenn dieser Link wieder auf einer stark frequentierten Forenseite wie „wallstreet-online“ gepostet wird? Die Konsequenzen für den Anbieter der verwundbaren Webseite möchte man sich besser nicht ausmalen.

Bild 3: Beispiel für Cross-Site Scripting



Maßnahmen: Die beste Möglichkeit, XSS-Attacken zu verhindern, ist ebenso wie bei B1 gefordert, die vollständige Validierung aller Nutzereingaben. Dringend anzuraten ist auch hier der Einsatz von Positivlisten, da es unzählige Wege gibt, HTML-Eingaben zu kodieren. Eine sinnvolle Möglichkeit zur Vermeidung von XSS-Attacken ist die Konvertierung von HTML-Tags, beispielsweise anhand der Tabelle 1:

Von	Nach
<	<
>	>
(	(
)	)
#	#
&	&

B5:
Buffer Overflows

Buffer Overflows betreffen potentiell alle Komponenten einer Webanwendung und können von verheerender Wirkung für die Integrität einer Anwendung sein, da die erfolgreiche Ausnutzung eines Buffer Overflows in der Ausführung beliebigen Codes auf dem betroffenen System resultiert. Meist sind Buffer Overflows und auch Format String-Schwachstellen aber nicht spezifisch für die eingesetzte Anwendung, sondern generisch für eine oder mehrere der eingesetzten Komponenten.

Buffer Overflows und Format Strings betreffen hauptsächlich C-Code, andere Programmiersprachen sind prinzipiell nicht von dieser Form von Schwachstellen betroffen, es sei denn, sie greifen auf in C geschriebene Bibliotheken zurück. Dies trifft beispielsweise auch auf die Programmiersprache Java zu, der ja häufig nachgesagt wird, dass Buffer Overflows hier nicht auftreten können. Übersehen wird dabei, dass die Java Virtual Machine (JVM), die für die Ausführung von Java Code benötigt wird, in C geschrieben ist. In den JVMs einiger Hersteller wurden auch bereits Buffer Overflows identifiziert.
Maßnahmen: Man muss davon ausgehen, dass in vielen Komponenten einer Webanwendung noch unentdeckte Buffer Overflows oder Format String-Schwachstellen auf ihre Entdeckung warten. Es sollten daher alle zur Verfügung stehenden Informationsquellen, wie die Security-Webseiten der Hersteller oder Mailinglisten wie Bugtraq (www.securityfocus.com) auf die Veröffentlichung neuer Schwachstellen überwacht werden. Wie verbreitet Buffer Overflows sind, zeigt ein Blick auf die gravierendsten Schwachstellen der letzten Monate: die Mehrzahl ist auf Buffer Overflows zurückzuführen. Ob die eigene Webanwendung hiermit behaftet ist, lässt sich nur durch Security-Scanner oder besser noch durch sorgfältigen Code-Review ermitteln. Um potentielle Buffer Overflows zu vermeiden, ist wieder einmal die Validierung aller Nutzereingaben erforderlich, besonderes Augenmerk ist hier auf die Längenprüfung der Eingaben zu lenken.

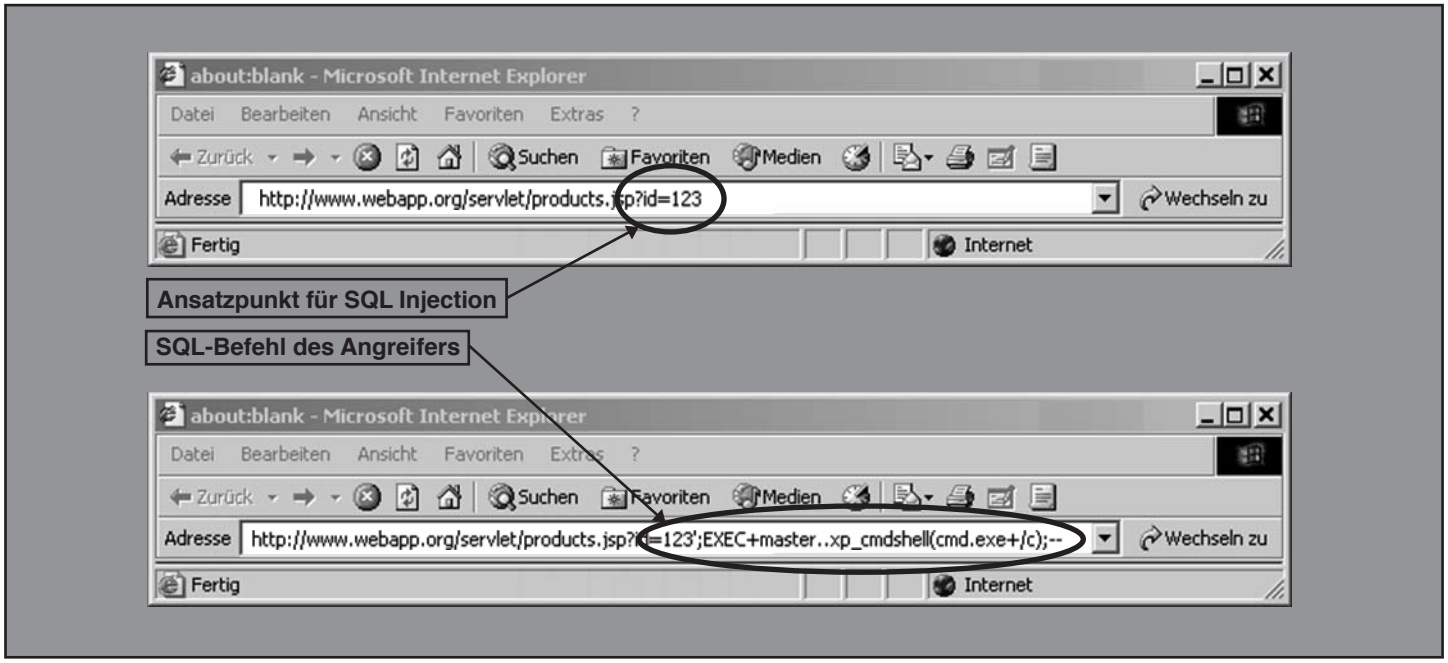
B6:
Einschleusen von Befehlen

Viele Webanwendungen nutzen Features des Betriebssystems oder anderer externer Programme, um bestimmte Funktionen zu ermöglichen.

Ein klassisches Beispiel ist hier der Aufruf des sendmail-Programms zum Versand von E-Mails aus der Anwendung heraus. Übergibt eine Anwendung Befehle an externe Programme aus den Daten einer HTTP-Anfrage, müssen diese sorgfältig überprüft werden. Geschieht dies nicht, kann ein Angreifer über das Einschleusen bestimmter Meta Charakter, den Kommandoaufruf modifizieren, oder im schlimmsten Fall eigene Kommandos zur Ausführung bringen.

Diese externen Befehle können über System Calls, die Nutzung externer Programme oder über das Datenbank-Backendsystem (via SQL) eingeschleust werden. Eine besonders verbreitete Form der Einschleusung externer Programme ist die so genannte SQL-Injection, die durch die fehlende oder fehlerhafte Prüfung von SQL-Befehlen eines Klienten ermöglicht wird. Die Folgen eines erfolgreichen SQL-Injection-Angriffs können beispielsweise die Modifikation Ihrer Webseite, die Kompromittierung sensibler Daten oder – bei bestimmten Datenbankservern – auch die Ausführung beliebiger Systembefehle sein.

Bild 4: Beispiel für SQL-Injection



Maßnahmen: Die beste Methode, das Einschleusen von Kommandos zu verhindern, ist die Vermeidung aller Aufrufe von externen Kommandos oder Systemcalls. Häufig können über Features der eingesetzten Sprache dieselben Resultate erreicht werden. In Bereichen, bei denen sich dies nicht vermeiden lässt – wie beispielsweise bei SQL-Abfragen – tritt wieder die Validierung aller übergebenen Parameter auf den Plan, zusätzlich kann auch über die Anwendung sog. Stored Procedures ein verbessertes Schutzniveau erreicht werden, da so nur der Zugriff auf die Daten gewährt wird, die auch wirklich innerhalb der Anwendung benötigt werden.

Eine weitere empfehlenswerte Schutzmaßnahme ist die konsequente Anwendung des Least Privilege Prinzips: Die Anwendung sollte also nur die Privilegien erhalten, die zwingend für deren Nutzung benötigt werden. Eine häufig anzutreffende Fehlkonfiguration ist der Datenbankzugriff als "sa"- (MS-SQL) oder DBADMIN- (Oracle) User, der Vollzugriff auf alle Datenbankinhalte hat.

Wenn externe Kommandos unbedingt gebraucht werden, müssen alle durch den Anwender hinzugefügten Informationen streng kontrolliert werden.

B7: Unzureichende Handhabung von Anwendungsfehlern

Nicht abgefangene Fehlermeldungen einer Anwendung können einem Nutzer mit bösartigen Absichten genaue Einsicht in deren Funktionsablauf erlauben. Häufig trifft man beispielsweise auf Datenbankzugriffsfehler – insbesondere bei ASP- und PHP-Anwendungen – oder Null Pointer Exceptions, mit kompletter Ausgabe des Stacks. Diese Ausgaben haben für den normalen Anwender keinen substanziellen Wert, sondern tragen eher zu dessen Verwirrung bei. Ein Angreifer kann sich so hingegen Stück für Stück durch die Anwendung tasten und die so gewonnenen Informationen in einem späteren Angriff nutzen.

Maßnahmen: Fehler in einer Anwendung sollten auch in dieser abgefangen werden. Ausgegeben werden sollte nur eine Meldung, die es einerseits dem Nutzer ermöglicht, Schlüsse daraus zu ziehen, was den Fehler verursacht hat und wie er sich nun verhalten soll, andererseits aber einem Angreifer keine Möglichkeit bietet, die genaue Applikationslogik zu identifizieren.

Im Zweifellsfall kann auch nur eine Standard-HTTP-Fehlermeldung wie 404 (File not Found) oder 403 (Forbidden) ausgegeben werden.

Verfügt die Webanwendung sogar über die Möglichkeit, wiederholte Fehlversuche zu registrieren, dann bietet sich hier eine Möglichkeit der frühzeitigen Erkennung von Angriffsversuchen.

B8: Unzureichende Nutzung von kryptographischen Methoden

Viele Webanwendungen müssen sensible Daten verarbeiten und speichern. Hier kann es sich beispielsweise um Passwörter, Kreditkartennummern oder auch Sozialdaten handeln, die keinesfalls ungeschützt im Internet veröffentlich werden dürfen.

Die Anwendung von kryptographischen Methoden zum Schutz von Daten ist heute beinahe zur Selbstverständlichkeit geworden, nichtsdestotrotz gibt es auch hier viele Möglichkeiten, etwas falsch zu machen.

Beispiele sind:

- Fehlerhafte oder unvollständige Verschlüsselung sensibler Daten
- Unsichere Speicherung von Schlüsseln, Zertifikaten und Passwörtern
- Deterministische Zufallsgeneratoren
- Unzureichende Verschlüsselungsalgorithmen (Base64 ist keine Verschlüsselung!)
- Erfinden eigener Algorithmen
- Keine Integration von Managementfunktionen (z.B. für Schlüsseltausch)

Maßnahmen: Die beste Methode Fehler bei der Nutzung von kryptographischen Methoden zu vermeiden, ist Kryptographie nur dort einzusetzen, wo sie auch wirklich benötigt wird.

Ausreichend getestete Verschlüsselungsalgorithmen gibt es zur genüge, daher ist es nicht sinnvoll, das Rad neu zu erfinden und einen eigenen Algorithmus zu kreieren.

Report zum Thema

Web-Browser

Sicherer Browser-Einsatz im Web

Der Report gibt einen Überblick über die gebräuchlichen Web-Technologien und Programmiersprachen und beleuchtet deren Sicherheitsmodelle. Die beim Surfen im Internet bestehenden Risiken werden detailliert beschrieben, bewertet und Lösungsszenarien mit den Sicherheitszielen Vertraulichkeit, Verfügbarkeit und Integrität der Daten aufgezeigt.

Web-Browser -Report
April 2003
264 Seiten
Preis: € 298,-- zzgl. MwSt.

Bestellen Sie auf unserer Web-Seite
www.comconsult-research.com

B9:
Denial-of-Service Angriffe (DoS)

Wegen starker Zunahme entsprechender Vorkommnisse ist dieser Punkt in 2004 neu aufgenommen worden. Auch Webanwendungen sind prinzipiell anfällig gegen DoS-Angriffe, da sie kaum unterscheiden können zwischen massiver Nutzung durch reguläre Anwender und massiver Störung durch Angreifer. Handelt es sich dabei um einen Distributed DoS, dann bietet auch die IP-Adresse des Aussendenden kein Erkennungskriterium.

Die Möglichkeiten per DoS-Angriff die reguläre Nutzung einer Webanwendung zu beeinträchtigen oder sogar vollständig zu unterbinden sind stark abhängig von der Anwendung selber. Bevorzugte Ziele sind Ressourcen, die sich mit einfachen Mitteln stören lassen und maximalen Erfolg versprechen. Hierzu gehören Überfluten der verfügbaren Bandbreite, der möglichen Datenbank-Verbindungen, des Plattenplatzes, der Prozessressourcen und der anwendungsspezifischen Ressourcen.

Maßnahmen: Eine perfekte Abwehr von DoS-Angriffen gibt es nicht, sie sollten aber zumindest erschwert werden. Zunächst sollten alle Ressourcen, die Anwendern zur Verfügung gestellt werden, auf das Notwendigste begrenzt sein. Nach erfolgreicher Authentisierung eines Anwenders können diesem dann je nach Einstufung auch weitergehende Ressourcen zugeteilt werden. Nicht authentisierte Anwender sollten keine Möglichkeit haben, unnötige Zugriffe auf Datenbanken oder andere limitierte Ressourcen durchzuführen.

B10:
Unsichere Konfiguration der Server

Webserver und Applikationsserver spielen eine entscheidende Rolle für die Sicherheit oder Unsicherheit der gesamten Anwendung. Ein Großteil der erfolgreichen Angriffe auf Webanwendungen hat meist triviale Ursachen, beispielsweise weil vergessen wurde, bestimmte sensible Dateien aus dem Webroot-Verzeichnis des Web- oder Applikationsserver zu entfernen. Zumeist sind auch unterschiedliche Mitarbeiter mit der Entwicklung bzw. der Betreuung einer Webanwendung betraut. Die sichere Bereitstellung einer Webanwendung erfordert jedoch das Know-how und die Mitwirkung aller Beteiligten.

Typische Probleme, die bei der Server-Konfiguration anzutreffen sind:

- Fehlende Security Patches
- Fehlerhafte Konfiguration der Server-Software (erlaubt beispielsweise die Aktivierung von Verzeichnislistings)
- Nicht benötigte Backup- oder Beispieldateien mit Scripts oder Webseiten
- Kritische Dienste sind aktiv, z.B. für Content Management oder Remote Administration
- Standardnutzerkonten ohne oder mit Standardpasswörtern
- Unzureichende SSL-Konfiguration (z.B. Nutzung von schwacher Verschlüsselung)
- Nutzung von Default-Zertifikaten und selbst signierten Zertifikaten
- Unzureichende Authentisierung

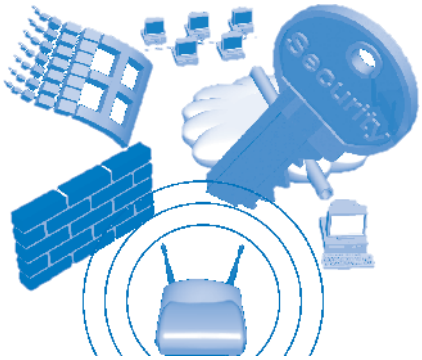
Einige dieser Probleme sind leicht mit Security-Scannern zu entdecken und anschließend auszunutzen. Die Folgen können beträchtlich sein, da die mögliche Kompromittierung nicht „nur“ den Webserver betrifft, sondern sich bis auf die Backend-Server und das interne Netzwerk erstrecken kann.

Maßnahmen: Für so gut wie alle Komponenten im Bereich Webanwendungen existieren detaillierte Anweisungen zum Security-Hardening, entweder von den Herstellern selber oder von Sicherheitsorganisationen wie OWASP, CERT oder SANS.

Grundsätzlich sollten aber die folgenden Punkte beachtet werden:

- Aktivierung aller eingebauten Sicherheitsmechanismen
- Deaktivierung aller nicht benötigten Serverkomponenten
- Aktivierung aller Rollen, Rechte, Accounts und Deaktivierung aller Default-Accounts
- Aktivierung von Logging- und Alarmierungsmechanismen
- Überwachung aller relevanten Informationsquellen auf das Auftauchen neuer Sicherheitslücken
- Regelmäßiges Einspielen von Security Patches
- Regelmäßige Durchführung von Schwachstellentests (intern, extern)

Seminar zum Thema



Sicherheits-Lösungen: Planung und praktische Konfiguration

Praxis-Seminar

19.04. - 23.04.04 Aachen
19.07. - 23.07.04 Aachen

Dieses Praxis-Seminar vermittelt den praktischen Umgang mit Firewall, VPN, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt. Als Übungsbasis stehen typische Produkte des Marktes zur Verfügung
Referenten: Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hans-Peter Mohn, Christian Osterbrink und Alexander Zarenko
Einzelpreis: € 2.290,-- zzgl. MwSt.

Buchen Sie über unsere Web-Seite **www.comconsult-akademie.de**

Maßnahmen zum Schutz von Webanwendungen

Neben den konkreten Hinweisen zur Abwehr der gerade vorgestellten häufigsten Schwachstellen von Webanwendungen gibt es einige grundlegende Maßnahmenpakete, die unbedingt beachtet werden sollten:

M1: Basistopologie für sichere Webanwendungen

Webanwendungen sollten immer in mehrstufiger Topologie (multi-tier) aufgebaut werden, um damit Angriffsmöglichkeiten deutlich zu erschweren. Dabei sind die funktionalen Anwendungs-Ebenen (Presentation-, Application-, Data-Layer) unbedingt auch physisch voneinander zu trennen, indem man voneinander separierte Server verwendet, die über gesicherte Verbindungen miteinander kommunizieren.

Es sollten zumindest die folgenden Komponenten unterschieden werden:

• Webbrowser (auf einem remote Desktop)

Dem Webbrowser kommt in einer Webanwendung die Rolle des Clients zu. Zum Einsatz kommen hier beispielsweise der Internet Explorer, Netscape / Mozilla oder Opera. Die Einflussmöglichkeiten des Anbieters von Webanwendungen auf solch entfernte Systeme werden zumeist sehr begrenzt sein. Es sollte aber unbedingt darauf hingewirkt werden, dass eine möglichst aktuelle Browserversion verwendet wird. Durch schwache Sicherheitsvorkehrungen auf dem Desktop ist das Einschleusen von Viren oder Trojaner eine stete Gefahr und kann dazu führen, dass unautorisiert auf persönliche Daten zugegriffen wird. Deshalb sollten den Nutzern zumindest Sicherheitshinweise gegeben werden, besser wäre natürlich der Einsatz von Sicherheitstools zum Schutz des Desktops: Virenscanner, Integritätschecker, Personal Firewalls. Spätestens bei Zugriff auf sensible Daten sollte unbedingt ein sicheres Authentisierungsverfahren und eine Verschlüsselung z.B. mit SSL (Secure Socket Layer) gewählt werden.

• Webserver

Je nach Komplexität und Aufbau einer Webanwendung kommt dem Webserver zumeist die Rolle des Front-Ends zur eigentlichen Anwendung zu. Webserver müssen wegen ihrer direkten Erreichbarkeit im Internet ein möglichst hohes Sicherheitsniveau aufweisen. Hierzu sind alle überflüssigen Module zu entfernen und das gesamte System ist einem „Hardening“ (Betriebssystem und eigentlicher Webserver) zu unterziehen. Es muss ständig auf einem aktuellen Stand (Version, Patches) gehalten werden, um keine altbekannten Sicherheitslücken anzubieten. Dieser Stand ist periodisch durch Security-Scanner zu überprüfen. Es empfiehlt sich auch, den Einsatz eines hostbasierten IDS/IPS-Systems einzuplanen. Die Positionierung eines Webservers in einem, durch Firewall kontrollierten Server-Segment verbessert die Sicherheit deutlich. Bei Einsatz von SSL bildet der Webserver den Endpunkt der gesicherten Kommunikation mit dem Client. Es ist deshalb für einen sehr guten Schutz des hierfür benötigten Private Keys zu sorgen.

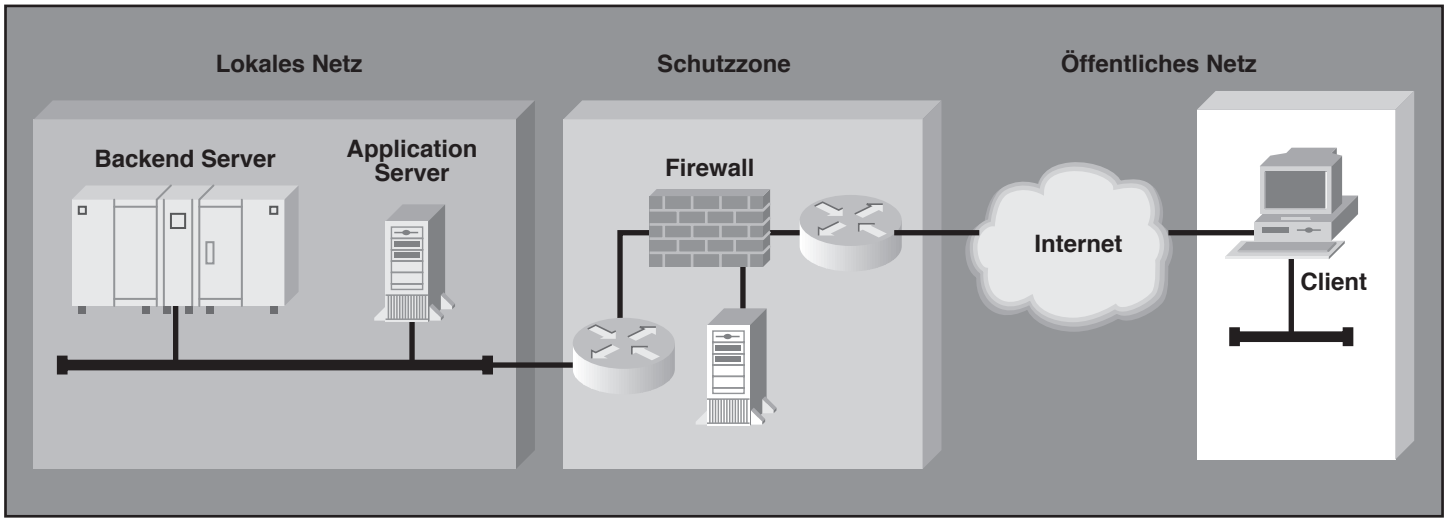
• Web-Applicationserver

Jeder Betrieb von zusätzlichen Anwendungen auf dem Webserver erhöht das Risiko des Eindringens über Schwachstellen dieser Software. Unbedingt zu empfehlen ist deshalb die Ausgliederung der eigentlichen Anwendungslogik auf einen zusätzlichen Web-Applicationserver, der gesichert im lokalen Netz steht und nur über einen gut überwachten Kommunikationskanal mit dem Webserver kommuniziert. Es wird empfohlen, auch diese (interne) Verbindung per SSL zu sichern. Der Web-Applicationserver ist das eigentliche Herzstück jeder Webanwendung. Den Markt teilen sich hier Hersteller wie BEA (Weblogic), IBM (WebSphere), Novell (exteNd) und Oracle Internet Application Server. Bei Risikoanalysen ist auch die Art der Kommunikation zwischen Web- und Web-Applicationserver genauer zu untersuchen. Handelt es dabei um eine ungeprüfte Weitergabe aller Nutzereingaben oder findet bereits auf dem Webserver eine Validierung statt?

• Backend-Server

Jede Webanwendung benötigt eine zentrale Ablage für die bereitgestellten Daten. Hier kommt als Backend in erster Linie ein Datenbankserver zum Einsatz. Die Auswahl dieses Servers ist meist in Kombination mit Webserver und Applikation gewählt, beispielsweise anhand des LAMP (Linux, Apache, MySQL, PHP) Modells. Ähnliches gilt auch für die Microsoft-Produktwelt, hier ist eine häufig anzutreffende Kombination der IIS, eine ASP-Anwendung und ein MS-SQL-Server als Backend. Die Kommunikation mit dem Web-Applicationserver sollte ebenfalls durch SSL geschützt werden, wenn dies auch bei rein interner Kommunikation als notwendig erachtet wird.

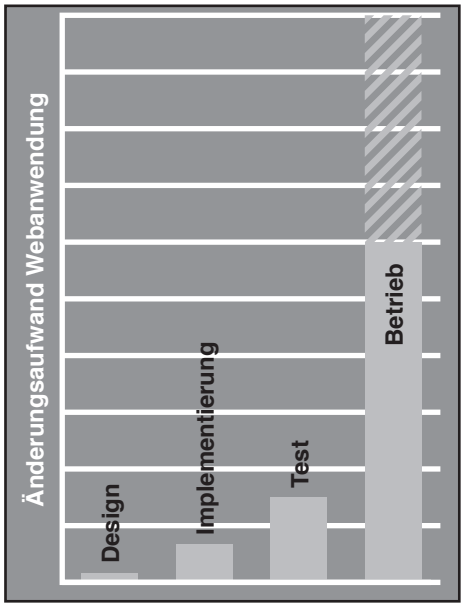
Bild 6: 3-tier Topologie einer Webanwendung



M2: Sicherheitsmaßnahmen bei neu erstellten Webanwendungen

Wie auch aus den TOP-10 Bedrohungen zu ersehen ist, stellt die ungenügende Beachtung von Sicherheitsaspekten bei der Programmierung von Webanwendungen das wohl größte Problem dar. Die „typischen" Entwickler besitzen in aller Regel kein ausreichendes Know-how in Sicherheitsfragen und werden zur Beachtung derselben leider auch allzu selten von ihren Auftraggebern angehalten. Sicherheitsrichtlinien oder Sicherheitskonzepte für die Anwendungsentwicklung existieren bei den wenigsten Unternehmen. Berücksichtigt man noch den Zeitdruck, unter dem die meisten Anwendungen entwickelt werden, dann kann man sich das Ergebnis gut vorstellen. Webanwendungen sind wegen ihrer verteilten Struktur und der verwendeten modernen Techniken zudem äußerst komplex. Bei komplexen Anwendungen muss aber auch immer mit einer gewissen Basisrate von Programmierfehlern gerechnet werden, Erfahrungswerte liegen bei ca. einem Fehler pro 1500 Zeilen Code. Damit bieten sich Angreifern eine Vielzahl von Möglichkeiten Webanwendungen erfolgreich zu attackieren, sei es wegen fehlender Sicherheitsmaßnahmen oder durch das Ausnutzen von Programmierfehlern.

Berücksichtigt man, dass nachträgliche Änderungen am Code einer Webanwendung immer aufwändiger werden (Design = 1, Implementierung = 6.5, Test = 15, Betrieb = 60 bis 100, Quelle: IBM Systems Sciences Institute) und wohl niemand lange mit Sicherheitslücken leben will, dann muss das Thema Sicherheit so früh wie möglich angegangen werden.



In den einzelnen Entwicklungsphasen sind folgende Punkte zu beachten:

• Designphase

– Einbeziehen von Sicherheitsspezialisten beim Systemdesign
– Formulierung eines Sicherheitskonzeptes
– Sensibilisierung / Training der Entwickler
– Etablieren von Security-Checks in den QA-Prozess
– Möglichst keine Verwendung „unsiche-rer" Sprachen (C, C++, Perl, VBA)
– (Auch serverseitig) keine ActiveX-Con-trols nutzen
– Implizites Starten anderer Anwendungen (z.B. MS Office) vermeiden / verhindern
– Keine „selbst entwickelten" Verschlüsselungsalgorithmen einsetzen
– Design granularer Anwendungen mit erforderlichen Zugriffsrechten
– Zusammenfassen aller Zugriffsregelungen in einem Security-Layer

• Implementierungsphase

Eine gute Basis für die Erstellung von Programmierrichtlinien liefert die OWASP mit der bereits erwähnten Top-10 Liste und dem „Guide to Building Secure Web Applications". Man erleichtert sich in dieser Phase das Leben deutlich, wenn man als Entwicklungs- und Ablaufumgebung einer Webanwendung einen J2EE Web Application Server einsetzt. Neben unbestreitbaren Vorteilen bei der Entwicklung selber (Java2-Technologie, Session- und Transaktionsmanagement, Skalierbarkeit usw.) wird auch die Umsetzung eines Sicherheitskonzeptes gut unterstützt (Funktionen für Authentisierung, Autorisierung, Verschlüsselung usw.).

• Test- und Betriebsphase

Neben den funktionalen Tests der Webanwendung ist aus Sicherheitssicht besonders die Schwachstellenanalyse interessant. Durch den Einsatz darauf spezialisierter Security-Scanner (ISS, Sanctum, Kavado, SPI Dynamics) können frühzeitig Angriffspunkte erkannt und beseitigt werden. Es empfiehlt sich aber immer noch, auch manuell durchgeführte Tests einzusetzen, da auch die besten Tools den aktuellen Entwicklungen immer einige Zeit hinterherlaufen und nicht immer über die benötigte Kontrolltiefe verfügen. Diese Schwachstellentests sollten auch im späteren Betrieb periodisch durchgeführt werden, da neue erfolgreiche Angriffsformen nie auszuschließen sind.

M3: Sicherheitsmaßnahmen bei vorhandenen Webanwendungen

Jede Webanwendung sollte wegen ihres hohen Gefährdungspotentials einer Risikoanalyse unterzogen werden.

Wurde sie im eigenen Hause unter Beachtung einer (abgenommenen) Sicherheitskonzeption erstellt, dann kann man sich im Wesentlichen auf die Prüfung der sachgerechten Umsetzung und des Betriebs konzentrieren.

Handelt es sich aber um eine zugekaufte Anwendung, dann stellt sich dieser Vorgang schon deutlich schwieriger dar. Eine Codeanalyse ist sehr aufwendig und wird auch wegen fehlendem Zugriff auf den Quellcode nur selten möglich sein. Hier muss man sich mit der Analyse der Dokumentation und Konfiguration begnügen, deshalb kommt der nachfolgenden Schwachstellenanalyse mit den bereits erwähnten Techniken (Security-Scanner, manuelle Tests) eine besondere Bedeutung zu.

M4: Sicherung durch externe Gateways

Ist die umgehende Beseitigung von Schwachstellen einer Webanwendung nur verzögert oder gar nicht möglich (Kaufanwendung), dann kann man diese nur noch mit dem Einsatz einer Application-Firewall (auch Application-Proxy) schützen. Diese Systeme werden als Gateway zwischen externer Welt und Webserver/Webanwendung platziert und kontrollieren den HTTP- Datenstrom auf bösartige Inhalte.

So wie die Enterprise-Firewall den Unternehmenszugang schützt, bewacht die Application-Firewall den Zugang zu Webserver und Webanwendung. Neben den natürlich notwendigen Filtermöglichkeiten auf bekannt bösartige HTTP-Requests ist den individuellen Konfigurationsmöglichkeiten der Application-Firewall eine hohe Bedeutung beizumessen. Nur mit einer Fähigkeit „reguläre" von „irregulären" Eingaben zu unterscheiden, kann man auch heute noch nicht bekannten Angriffstechniken halbwegs beruhigt entgegen sehen.

Hierfür sind aber Lerntechniken einzusetzen, die anwendungsspezifisch arbeiten können und keinen zu hohen Bearbeitungsaufwand erfordern.

Webanwendungen: Die neue Hintertür ins Unternehmen?

In letzter Zeit haben diverse Hersteller Produkte zum Schutz von Webanwendungen angeboten. Die interessantesten darunter sind:

- Seclutions mit AirLock

  setzt auf eine eigene hochsichere Betriebssysteminstallation auf Basis von mitinstalliertem Solaris auf. Um Attacken gegen Webanwendungen zu verhindern, werden Filtertechniken eingesetzt. Diese Filter werden pro Anwendung eingeschaltet und können für bestimmte URLs deaktiviert werden. AirLock unterstützt eine zentrale Benutzerauthentisierung und die gängigen Authentisierungsserver (LDAP, Radius, ACE), um unabhängig von den Anwendungen eine Benutzerauthentisierung durchzusetzen. AirLock kommt ohne Lernphase aus und ist entsprechend leicht zu konfigurieren. Die Basisfilter bieten aber trotzdem einen recht umfassenden Schutz. (www.seclution.ch/en/ct_products_en.htm)

- Kavado mit InterDo

  …bedient sich eines so genannten „Positiven Sicherheitsmodells". Alle Daten von und zu den überwachten Webanwendungen werden überprüft. Nur erlaubte Anfragen/Antworten werden durchgelassen. Für diese „Whitelist" sind umfangreiche und an die Anwendung angepasste Regelsätze notwendig. Zur Erstellung dieser Regelsätze bietet InterDo diverse Möglichkeiten wie manuelle Eingabe, Lernmodus, Autopolicy usw. (www.kavado.com/ProductsInterdo.htm)

- Sanctum mit Appshield

  …bezieht sich auf ein Positives Sicherheitsverfahren mit dem Namen Dynamic Policy Reccoginition Engine (DPRE). Die DPRE analysiert permanent den Verkehr zwischen Client und Server. Durch diese Analyse der ausgehenden Daten kann die DPRE dynamisch entsprechende Regeln generieren und so nur gültige Antworten des Clients an den Server durchlassen. Zusätzlich überprüft AppShield die Integrität der URLs, Cookies und Hidden Fields. Die Basiskonfiguration beschränkt sich auf die Definition der erlaubten Start-URLs. Dieser sich daraus ergebende Schutz wird von Sanctum als Basic-Security bezeichnet. Für weitergehenden Schutz der Webanwendung wird auch bei AppShield eine Lernphase und Anpassungsphase benötigt. (www.sanctuminc.com/solutions/appshield /index.htm)

Ein nicht-kommerzielles Beispielprodukt ist Codeseeker des OWASP-Projekts. Codeseeker war ehemals ein kommerzielles Produkt der Firma Butterfly Security und wurde im November 2002 dem OWASP-Projekt übergeben. Mittlerweile ist die erste öffentliche Beta-Version erschienen, zu finden unter: www.owasp.org/development /codeseeker/. Der erste Eindruck ist hier durchaus positiv, es bleibt zu hoffen, dass die zuletzt schleppende Weiterentwicklung des Tools zukünftig intensiviert wird.

Auch mit anderen frei verfügbaren Tools kann bereits ein wesentlich verbessertes Schutzniveau einer Webanwendung erreicht werden. Nutzer des Internet Information Servers sollten in jedem Fall einen Blick auf das freie Tool URLScan (www.microsoft.com/technet/security/tools /tools/urlscan.asp)) werfen, das ebenso wie auch die kommerziellen Tools per White- oder Blacklisting-Verfahren (fast) beliebige Filter auf HTTP-Header-Ebene zulässt. Im Zusammenspiel mit anderen freien Tools wie ISAPI Rewrite (www.isapirewrite.com), das per Regular Expressions noch weitergehende Filterregeln ermöglicht, kann zumindest bei Anwendungen von einfacher bis mittlerer Komplexität ein im Vergleich zu den erstgenannten kommerziellen Tools gleichwertiges Schutzniveau erreicht werden. Eine zentrale Verwaltung der Filter und Logdateien kann mittels URLScan und isapirewrite allerdings nicht ermöglicht werden.

Fazit

Der Betrieb von Webanwendungen führt bereits heute zu den größten Sicherheitsrisiken für Unternehmen, die sich dieser Gefahren aber nur langsam bewusst werden. Durch neu aufkommende Techniken wie Web-Services wird diese Problematik in den nächsten Jahren eher noch gesteigert werden, deshalb sollte man sich beizeiten damit beschäftigen. Bei Eigenentwicklungen können einfache Programmierrichtlinien bereits die größten Schwachstellen von Beginn an vermeiden. Zusätzlichen Schutz liefern dann Produkte aus dem aufkommenden Markt der Application-Firewalls.

Eine ausführliche Abhandlung zu „Web-Services und Security" findet sich auch in der Ausgabe 10 des Security Journals (www.gai-netconsult.de/journal)

NEW **Security** Journal NEW

– Aktuelle Informationen zum Aufbau sicherer eBusiness Lösungen –

Der kostenfreie Service der GAI NetConsult GmbH erscheint alle zwei Monate mit aktuellen, sorgfältig recherchierten Informationen aus der Welt der IT-Security.

Mit unseren Erfahrungen aus vielen Security-Projekten wollen wir den Lesern helfen, "typische" Fehler zu vermeiden und durch erweitertes Know-how auch neue Themen effizienter angehen zu können. Jede Ausgabe enthält mindestens zwei **Fachartikel** zu Themen aus Technik und Management. In einer "TOP 10 der **Sicherheitsrisiken**" stellen wir die unserer Ansicht nach wichtigsten Bedrohungen der letzten zwei Monate zusammen. Auf diese sollte man unbedingt durch die empfohlenen Gegenmaßnahmen reagieren. Im fortlaufenden "**News Ticker**" finden sich interessante Nachrichten zum Thema Security.

EIN SERVICE DER

GAI NetConsult

Die **GAI NetConsult GmbH** konzentriert sich als System- und Beratungshaus auf die Planung und Realisierung von sicheren eBusiness Lösungen. Dabei wird der gesamte Prozess von der Analyse über die Konzeption und Realisierung bis zur Überwachung angeboten.

WEITERE INFORMATIONEN FINDEN SIE UNTER www.gai-netconsult.de

Fachartikel der letzten Ausgaben

Zentrales Mail-Gateway als virtuelle Poststelle
Einfache Möglichkeit für Unternehmen eine gesicherte Email-Kommunikation mit zentral administrierter Verschlüsselung und Signierung aufzubauen.

Instant Messaging - die neue Bedrohung?
Die Risiken bei der Nutzung von Instant Messaging (IM) sind weitgehend unbekannt. Dieser Artikel schafft Abhilfe und beschreibt die notwendigen Schutzmaßnahmen.

Web-Services und Security
Beschreibung der Grundlagen von Web-Services und der relevanten Standards im Sicherheitsbereich. Sicherheitstechnologien unter Architekturgesichtspunkten.

Design sicherer Unix-Administrationsumgebungen
Projektergebnisse zum Aufbau einer sicheren Unix-Administration mit dem Einsatz von SSH und sudo für sichere Ende-zu-Ende- Verbindungen.

Wie viel darf IT Sicherheit kosten?
Darstellung und Bewertung von qualitativen und quantitativen Argumentationshilfen bei Investitionsverhandlungen zur IT-Sicherheit. Tools zur Berechnung von RoSI (Return-of-Security-Investment).

Rechtlich Maßnahmen zur Hackerabwehr
Aktuelle Rechtsgrundlagen zur Überwachung und Verfolgung von Hacker-Angriffen auf ein Unternehmen.

Verschlüsselte Dateiablage
Erfahrungsbericht zu einem Projekt über Verschlüsselungstechniken im Intranet.

Sicherheitsrisiko Internet Explorer ?
Vorstellung aktueller Sicherheitslücken und Empfehlungen zur sicheren Konfiguration des Internet Explorers.

SSL-Proxy: Gateway-Security trotz Verschlüsselung
Unterbrechung verschlüsselter Verbindungen, um auch diese einer zentralen Kontrolle auf Malware und Zertifikatsverwaltung unterziehen zu können.

KonTraG
Vorstellung der Anforderungen des KonTraG an den IT Risk Management Process. Ausführliche Diskussion der Phase: Risikoidentifikation.

SPAM-Abwehr: Was ist rechtlich und technisch machbar?
Rechtliche Grundlagen der SPAM-Abwehr und technische Möglichkeiten einiger konkreter Produkte werden vorgestellt.

Auf unserer Web-Seite können Sie ein Probe-Exemplar als pdf-Datei herunterladen. Bei dauerhaftem Interesse nehmen wir Sie gerne in unseren Verteiler auf. Lassen Sie sich einfach registrieren und Sie erhalten danach per Email die jeweils aktuelle Ausgabe als pdf-Datei zugesandt. Darüber hinaus erhalten Sie die aktuelle Version zum sofortigen Herunterladen.

FÜR IHR ABONNEMENT BESUCHEN SIE BITTE UNSERE WEB-SEITE

www.gai-netconsult.de/journal/

CCNE

ComConsult Certified Network Engineer

Lokale Netze
- 19.04. - 23.04.04 Aachen
- 14.06. - 18.06.04 Aachen

TCP/IP und SNMP
- 03.05. - 07.05.04 Berlin
- 05.07. - 09.07.04 Bonn

Internetworking
- 19.04. - 23.04.04 Aachen
- 21.06. - 25.06.04 Aachen

Ethernet Technologien – neuester Stand
- 28.06. - 02.07.04 Aachen
- 13.09. - 17.09.04 Aachen

Paketpreis für alle vier Seminare: € 7.780 ,-- zzgl. MwSt.
(Einzelpreise: je € 2.290,--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
- 26.04. - 30.04.04 Aachen
- 05.07. - 09.07.04 Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
- 10.05. - 14.05.04 Aachen
- 06.09. - 10.09.04 Aachen

Trouble Shooting für TCP/IP-und Windows-Umgebungen
- 29.03. - 02.04.04 Aachen
- 21.06. - 25.06.04 Aachen

Paketpreis für alle 3 Seminare mit
Etherreal und Fluke Nettool Inline:
€ 7.500,-- zzgl. MwSt. (Seminar-Einzelpreise: je € 2.490,--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
- 03.05. - 07.05.04 Zürich
- 24.05. - 28.05.04 Köln

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
- 22.03. - 24.03.04 Bonn
- 28.06. - 30.06.04 Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
- 19.04. - 23.04.04 Aachen
- 19.07. - 23.07.04 Aachen

Paketpreis: € 5.330,-- zzgl. MwSt.
(Einzelpreise: € 2.290,-- / € 1.690,-- / € 2.290,--)

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

Impressum

Verlag:
Dr. Suppan International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland, Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich, 12 Ausgaben im Jahr

Bezug:
Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie

Für unverlangt eingesandte Manuskripte
wird keine Haftung übernommen

Nachdruck, auch auszugsweise
nur mit Genehmigung des Verlages

© Dr. Suppan International Institute b.v.