securitytime
ZEITUNG DER IT-SICHERHEIT

Zeitung für
IT-Sicherheitsverantwortliche

Zweites Quartal 2003

Nr. 1/2003
Schutzgebühr
Euro 2,50

Bruce Schneier Chairman der IT-Defense 2004

Auch im nächsten Jahr findet die IT-Defense wieder statt

HEILBRONN/HEIDELBERG, im Juni 2003 – Einige der weltweit bekanntesten IT-Security-Experten haben sich vom 22. bis 24. Januar auf der IT-Defense 2003 in Leverkusen mit Vertretern der deutschen und europäischen IT-Sicherheitsszene getroffen.

Neben Bill Cheswick, dem Chairman der Veranstaltung, waren als Referenten unter vielen anderen Simon Singh, Simple Nomad, Hans-Jürgen Stenger, Ian Vitek und Stefan Strobel mit dabei. Themen wie „Die aktuelle und zukünftige Entwicklung der IT-Sicherheit“ wurden ebenso diskutiert wie „Welche Angriffe erwarten uns in den nächsten Jahren?“.

Die insgesamt 150 Teilnehmer waren vollauf begeistert von den Referenten, der Qualität der Vorträge und nicht zuletzt auch von der Location BayArena.

Die Möglichkeit des persönlichen Kennenlernens der Referenten und der Austausch unter Gleichgesinnten standen im Mittelpunkt der Veranstaltung. Die Hacking Area war ein ständiger Anlaufpunkt sowohl während der Vorträge als auch in den Pausen.

Nach dem Erfolg des ersten Kongresses, wird die IT-Defense im nächsten Jahr in neuer Umgebung wieder stattfinden. Viele der Teilnehmer hatten ihr Kommen für 2004 bereits zugesagt. Einige Branchengrößen, die dieses Jahr verhindert waren, haben sich als Referenten schon vormerken lassen.

weiter auf Seite 8

Bill Cheswick, Chairman der IT-Defense 2003 Seine Aufgabe wird Bruce Schneier bei der IT-Defense 2004 übernehmen.

editorial

Liebe Leserinnen
und Leser,

dies ist die erste Ausgabe der securitytime, einer im Zeitungsformat aufgemachten Publikation, über deren Herkunft und Ziele wir vorab ein paar Sätze sagen möchten.

securitytime ist kein neues verlegerisches Zeitschriftenprojekt. Es ist auch kein redaktionell verkleideter Werbeprospekt.

Entstanden ist die Idee unmittelbar nach der IT-Defense 2003 in Leverkusen, eine Konferenz, die sowohl uns, die Veranstalter, als offensichtlich auch die Teilnehmer überrascht hat, weil in diesen 3 Tagen enorm viele Diskussionen auch außerhalb der Vortragssessions entstanden sind. Die großen Namen der internationalen IT-Security-Szene haben nicht nur dort vorgetragen, sondern in vielen persönlichen Gesprächen mit Teilnehmern ihre Erfahrungen weitergegeben.

Angeregt durch diese offene Arbeitsatmosphäre auf der IT-Defense, wollten wir eine weitere Plattform schaffen, um informell und unkompliziert den Austausch von Informationen zum Thema IT-Sicherheit zu fördern.

Die redaktionellen Inhalte werden von einem Netzwerk von IT-Sicherheitsprofis und Autoren geliefert, die zusammentragen und schreiben, was für die Branche interessant sein könnte.

Wir hoffen sehr, mit der securitytime ein interessantes Medium für Sie geschaffen zu haben und würden uns über Ihr Feedback freuen.

Ihr

Stefan Strobel
cirosec GmbH

Gerhard Roßbach
dpunkt.Verlag

Stefan Middendorf zur Sicherheit von Web Services

Sicher bedient

Wer einen Web Service bereitstellt, schafft einen Angriffspunkt, den eine Firewall alleine nicht schützen kann. Administratoren und Entwickler müssen zusätzlich auf Anwendungsebene für Sicherheit sorgen.

Im Mittelpunkt der Diskussion über Web Services stehen meist die Technik selbst, ihre Perspektiven für die Integration oder die Auseinandersetzung, ob nun Java oder .Net besser sei.

Unabhängig von all dem muss man berücksichtigen, dass die unbedachte Bereitstellung eines Web Services Angreifern ganze Scheunentore öffnen kann. Angriffspunkte bieten einerseits die Infrastruktur (Angriffe gegen Webserver wie bei herkömmlichen Webapplikationen) und andererseits die Implementierung des Dienstes selbst.

Die Kommunikation zwischen Client und Server eines Web Services unterscheidet sich in zwei Punkten von klassischen Web-Anwendungen, bei denen ein Benutzer mit seinem Browser mit einem HTTP-Daemon interagiert:

- Web Services dienen selten der Interaktion mit einem Benutzer. Vielmehr steht die direkte Kopplung und Integration von Anwendungsservern, das heiflt die Kommunikation von Maschine zu Maschine, im Vordergrund. Dies erhöht das Sicherheitsrisiko, da Manipulationen an Transaktionen schnell bis in die Backend-Systeme durchschlagen.
- Die meisten Web Services verwenden zum Nachrichtenaustausch das Simple Object Access Protocol (SOAP), das meist über HTTP transportiert wird. SOAP-Nachrichten bestehen aus XML-Dokumenten, die Aufrufe und deren Parameter enthalten.

Eine Gemeinsamkeit mit klassischen Web-Anwendung besteht allerdings darin, dass Firewalls nichts gegen Angriffe auf Anwendungsebene ausrichten können. So stellt beispielsweise die Manipulation eines HTTP-GET- oder -POST-Parameters aus Sicht der Anwendung einen Angriff dar, aus Sicht der Firewall handelt es sich jedoch um eine legale HTTP-Transaktion über Port 80. Diese Unfähigkeit von Firewalls, Angriffe auf Anwendungsebene erkennen zu können, bezeichnet man als Port-80-Problem.

Schwachstellen von SOAP

SOAP bietet ähnlich wie HTTP keinen Schutz gegen Angriffe auf Anwendungsebene. So warnt die SOAP-Spezifikation des W3C: „The SOAP Messaging Framework does not directly provide any mechanisms for dealing with access control, confidentiality, integrity and non-repudiation.“

Mittlerweile gibt es jedoch einige Zusatzstandards, die diese Lücken schließen.

Eine SOAP-Nachricht besteht aus einem sogenannten Envelope, der seinerseits in Header und Body unterteilt ist. Zudem können an einer Nachricht Dateien als Attachment hängen. Die Transportmethode hängt vom Trägerprotokoll ab: Bei HTTP bilden Envelope und Attachment ein Multipart-POST, bei SMTP dagegen ein MIME-Attachment.

Der SOAP-Body besteht im Wesentlichen aus Nachrichten und deren Parametern. Beim Einsatz von SOAP als RPC-Mechanismus (Remote Procedure Call) tauschen die Teilnehmer in der Regel zwei Nachrichten aus: Eine stellt die Anfrage dar, und die zweite enthält als Antwort darauf den Rückgabewert. Der SOAP-Body ist hierbei vor allem auf zwei Arten verwundbar:

Ein Angreifer kann versuchen, Methoden aufzurufen, die nicht für seinen Zugriff gedacht sind, und er kann die Parameter manipulieren.

Die Anwendungen müssen deshalb die Reihenfolge und den Typ der übergebenen Parameter prüfen. Selbst dann können Angriffe durch Änderung der Parameterwerte erfolgen. So lässt sich die von herkömmlichen Web-Anwendungen bekannte SQL-Injection auf Web Services übertragen. ...

weiter auf Seite 3

markt & trend:
Buchtipp: Stefan Strobel
Firewalls und IT-Sicherheit

Dieses Buch gibt einen umfassenden Überblick über praktische IT-Sicherheit in Unternehmen. Es erklärt die Methoden der Hacker sowie die Konzepte und Produkte,...

markt & trend Seite 2

e-business:
Einstürzende Mauern

Technische IT-Sicherheitskonzepte, die in den letzten zehn Jahren von Firmen implementiert wurden, haben sich vor allem auf die Absicherung der Netzwerkgrenzen konzentriert.

e-business Seite 6

Alexander Geschonneck, Berlin

Den Beweis in der Hand – Computer Forensik bei PDAs

Forensische Untersuchungen nach Systemeinbrüchen auf Servern und Clients gehören mittlerweile zum Alltag von Sicherheitsspezialisten. Durch den Einzug von mobilen Handhelds in den privaten und geschäftlichen Alltag rücken auch diese Geräte in den Mittelpunkt der Aufklärung von möglichen Computerstraftaten. Digitale Forensik oder auch Computer-Forensik hat sich in den letzten Jahren für den Nachweis und die Ermittlung von Straftaten aus dem Bereich der Computerkriminalität durchgesetzt. In Anlehnung an die allgemeine Erklärung des lateinischen Wortes Forensik, ist die Digitale Forensik ein Teilgebiet, das sich mit dem Nachweis und der Aufklärung von strafbaren Handlungen z.B. durch die Analyse digitaler Spuren beschäftigt. Welche Schritte können durchgeführt werden um sicherzustellen, dass so viele Informationen wie möglich von einem kompromittierten System gesammelt werden können, wobei der aktuelle Zustand bzw. Status dieses Systems so wenig wie möglich verändert wird? Zur Beantwortung dieser scheinbar einfachen, aber in der Umsetzung recht komplexen Frage muss grundsätzlich geklärt werden:

- Wie wird der Angriff oder der Sachverhalt verifiziert?
- Wie sollte das kompromittierte System und die zugehörige Umgebung gesichert werden?
- Welche Methoden können für die Sammlung von Beweisen verwendet werden?
- Wo sucht man nach Anhaltspunkten und wie können sie gefunden werden?
- Wie kann das Unbekannte analysiert werden?

Pdd , PDA Seizure und andere Tools stehen zur Verfügung, um Daten von Palm PDAs oder Windows CE Handhelds zu kopieren bzw. zu analysieren. Aber auch einige der bereits für die klassische forensische Untersuchung von Festplattenimages verwendeten Tools können zur Analyse von PDA Images verwendet werden.

PalmOS, das Betriebssystem des Palm PDA und seinen Nachfolgern, ist von einigen Herstellern (u.a. Handspring, Sony, IBM, Kyocera, TRG) lizenziert worden und wird mit deren eigenen Geräten ausgeliefert. Die Analysesoftware für den klassischen Palm PDA kann in der Regel für alle diese Geräte verwendet werden. Es ist dabei nur zu beachten, über welche Schnittstellen man auf diese Systeme zugreifen kann. Ist der Zugriff auf ein Speicher-Image dieser PDAs möglich, können alle Applikationen und Datenbanken analysiert werden. Hierzu gehören u.a. Protokolldaten, Aufgabenlisten, als „privat“ gekennzeichnete Einträge, Passwörter,

kryptografische Komponenten, besuchte Webseiten und weitere für die Ermittlung wichtige Informationen. Zusätzlich können Datenbanken von bereits gelöschten Applikationen analysiert werden. In diesen Images finden sich weiterhin als gelöscht markierte Objekte, die aber erst beim nächsten Hotsync-Vorgang endgültig gelöscht werden. Selbst verschlüsselt gespeicherte Datenbanken liegen während der Laufzeit unverschlüsselt im Speicher. Hat man dann Zugriff auf diese Speichersegmente, sind alle diese Informationen grundsätzlich auch auslesbar.

Der Algorithmus zum Verschlüsseln des Userpassworts eines Palm PDA ist bis zur PalmOS Version 4 nicht ausreichend gegen Angriffe gesichert. Hat man Zugriff auf diesen verschlüsselten Text, kann man z.B. mit dem Tool palmdecrypt das Passwort entschlüsseln. So erhält man Zugriff auf die verschlüsselten Passwörter zum Beispiel über die „Unsaved Preferences“ Datenbank oder über einen Mitschnitt des seriellen oder Netzwerk-Verkehrs während des Hotsync-Vorganges.

```
D:\Programme\misc\forensic>palmcrypt -d
 841316826AAC5AB1395F2BEA247E6737796FC1D2428BE0213BA80F52C5FAB382D
PalmOS Password Codec
kingpin@atstake.com
@stake Research Labs
http://www.atstake.com/research
August 2000

0x67 0x65 0x68 0x65 0x69 0x6D          [geheim ]
```

Der BlackBerry ist ein sogenanntes allways-on Gerät, das Nachrichten über eine Push-Technologie übermittelt bekommt. Informationen werden über die GPRS-Funkverbindung ständig auf das Gerät gesendet. Dies bedeutet aber, dass die Spuren, die bereits gelöschte Daten hinterlassen haben, jederzeit unkontrolliert überschrieben werden können. Ohne „Vorwarnung“ können Applikationen wie der Email-Client, der Instant Messenger, der Wireless Calendar und alle weiteren zusätzlich installierten Tools Daten empfangen. Dadurch wird eine forensische Analyse erschwert. Diese Eigenschaft der BlackBerry-Geräte macht es erforderlich, den Funkempfang sofort zu deaktivieren, wenn man den ersten Zugriff auf ein zu untersuchendes Gerät hat. Ein Ausschalten ist in diesem Kontext nur bedingt empfehlenswert, da

der BlackBerry nur dann vollständig ausgeschaltet ist, wenn die Stromzufuhr für eine länger Zeit komplett unterbunden wurde oder das Gerät in den Storage Mode geht. Wenn es nur über das GUI ausgeschaltet wird, werden allerdings lediglich Display, Tastatur und Funkempfang deaktiviert. Wird das Gerät eingeschaltet nachdem es über das GUI ausgeschaltet oder vom Stromkreis abgeschnitten wurde, werden alle Informationen aus der Server-Queue per Funk auf den BlackBerry übertragen, noch bevor man die Chance hat, den Funkempfang zu deaktivieren. Nach einem kompletten Stromlosschalten des Gerätes findet beim folgenden Start ein System-Reset statt, der automatisch die meisten der für eine forensische Untersuchung interessanten Logfiles löscht und ein System-Cleanup durchführt. Dieses System-Cleanup hat den aus forensischer Sicht unerfreulichen Nachteil, dass der SRAM gelöscht bzw. Filesystem-Bereiche neu organisiert werden und damit Reste zuvor gelöschter Daten verloren gehen. Ein weiterer Stolperstein für Ermittler ist, dass der für eine Filesystem-Analyse benötigte System-Snapshot ebenfalls in einem System-Reset endet. Hier gilt es also genau zu überlegen, welchen Analyseschritt man zuerst durchführt. Mit Hilfe des BlackBerry SDK oder des Tools RIMWalker hat man dann Zugriff auf die installierten Datenbanken, Logfiles oder sonstige versteckte Dateien auf dem BlackBerry. Man sollte aber beachten, dass die dafür nötige serielle Kommunikation unter Umständen stromzehrend sein kann.

Es liegt auf der Hand, dass jede der oben aufgeführten Techniken und Methoden auch für die Analyse von gestohlenen oder anderweitig unberechtigt erlangten PDAs verwendet werden könnte. Sind sensible Informationen darauf gespeichert, wird der Besitzer nicht wollen, dass diese in fremde Hände gelangen. Wenn man sich aber nur auf die eingebauten Sicherheitsmechanismen verlässt, sind diese vertraulichen Informationen nicht lange geschützt. Hier sollten zusätzliche Sicherheitstools von Drittherstellern verwendet werden. Eine weitere hilfreiche – leider oft vergessene – Präventivmassnahme ist die Unterbindung des unberechtigten physischen Zugriffs durch geeignete sichere Aufbewahrung während des mobilen und auch stationären Einsatzes.

buchtipp

Stefan Strobel

Firewalls und IT-Sicherheit

3., aktualisierte und erweiterte Auflage -- iX Edition

Dieses Buch gibt einen umfassenden Überblick über praktische IT-Sicherheit in Unternehmen. Es erklärt die Methoden der Hacker sowie die Konzepte und Produkte, mit denen man sich vor ihnen schützen kann - unabhängig davon, ob ein Internet-Anschluss, ein Remote-Access-Zugang oder ein E-Business-System zu sichern ist.

Beispielhaft werden typische Lösungen vorgestellt und die Prinzipien erläutert, auf denen sie basieren. Der Leser kann damit verschiedene Vorgehensweisen bewerten und erhält Hilfestellung beim Aufbau seiner eigenen Sicherheitsumgebung.

Praxisnah werden u.a. folgende Themen dargestellt:

- Angriffsziele und -methoden sowie Schutzmaßnahmen
- Prinzipien, Anwendungsgebiete und Komponenten von Firewalls
- VPNs, Authentifizierung und Content-Security
- Konzepte und Produkte für Remote-Access und Partneranbindungen
- Erkennen von Angriffen / Intrusion Detection

In der 3. Auflage wurden die bestehenden Kapitel aktualisiert, neue Produkte aufgenommen sowie ein Kapitel zur Sicherheit von Web-Applikationen und E-Business hinzugefügt.

Das Buch eignet sich als Anleitung für IT-Verantwortliche und Administratoren, die ihre IT-Infrastruktur sicherer machen möchten, und als Entscheidungshilfe bei der Frage, welche der vielfältigen Security-Möglichkeiten im eigenen Unternehmen einzusetzen sind.

Zielgruppe:
IT-Sicherheitsverantwortliche, IT-Management Netzwerkverantwortliche, Systemadministratoren, Webmaster

Autor / Autorin:
Stefan Strobel ist Geschäftsführer der cirosec GmbH, einem Unternehmen, das sich ausschließlich dem Thema IT-Sicherheit widmet. Neben seiner Tätigkeit ist er Dozent an Berufsakademien und an der Fachhochschule Heilbronn, hält Vorträge auf Fachkongressen und ist Autor verschiedener Fachbücher, die in mehreren Sprachen erschienen sind.

Rezensionen:

- „...bietet einen guten Überblick über Konzepte, Anwendungen und Komponenten...“ (Screen Business Online zur 2. Auflage)
- „... eine qualitativ hochwertige und flüssig geschriebene Einführung in das Thema.“ (LANline Spezial, Das sichere Netz, zur 2. Auflage)
- „Ein durchweg empfehlenswertes Buch.“ (Internet Professionell zur 2. Auflage)
- „... insbesondere wegen des gut durchdachten Konzeptes ... ideal für Systemadministratoren und Entscheidungsträger.“ (Funkschau zur 2. Auflage)
- „Insgesamt ein sehr gutes Werk, das die Thematik knapp, aber vollständig abhandelt.“ (GUUG-Nachrichten zur 2. Auflage)
- „... guter Überblick über den Stand der Technik ... sachkundige und komprimierte Vorstellung von Produkten ...“ (Der Sicherheitsberater zur 2. Auflage)

iX Edition
3., aktualisierte und erweiterte Auflage
dpunkt.verlag
Dezember 2002
316 Seiten, Broschur
44 Euro (D) / 45,3 Euro (A) / 72 sFr
ISBN 3-89864-152-X

Fortsetzung von Seite 1

Die klassische Form dieser Attacke schleust SQL-Anweisungen über Eingaben in HTML-Formulare ein. Wenn eine Web-Anwendung eine Datenbankabfrage wie

```
SELECT Name FROM Artikel
WHERE Nummer=<Parameter>
```

durchführt, liefert sie den Namen eines Artikels zurück, wenn der Benutzer im Web-Formular eine Nummer einträgt. Gibt er dagegegen

```
123; DELETE from Artikel
```

ein, führt der Server die an das SELECT angehängte DELETE-Anweisung aus, falls die Anwendung das Eingabefeld nicht prüft. Ist der Parameter einer SOAP-Nachricht manipuliert, kann das denselben Schaden anrichten. An diesem Trivialbeispiel zeigt sich bereits, wie wichtig eine inhaltliche Prüfung und Filterung der Parameterwerte bei Web Services ist.

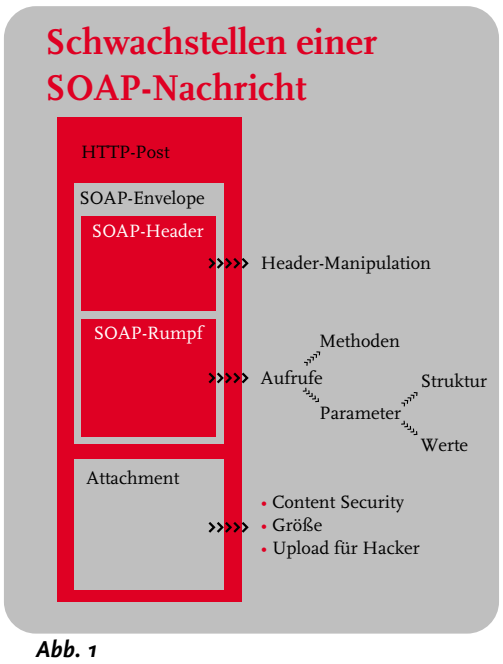


Abb. 1

Eine weitere Angriffstechnik ist das Erzeugen von Buffer Overflows. Dieses Verfahren basiert darauf, in Parametern Maschinencode einzuschleusen, der auf dem Zielsystem beispielsweise eine Shell startet. Das bedroht Komponenten, die in binärer Form vorliegen – etwa Module des Web Services oder nachgelagerte Dienste.

Bei in Java implementierten Web Services besteht das Risiko von Buffer Overflows prinzipiell bei Einbindung nativer Bibliotheken.

Bei einer „Pure Java"-Implementierung besteht diese Gefahr nicht, da die Laufzeitumgebung stets Längenprüfungen beim I/O durchführt. Analog gilt für .Net, dass das Einbinden vorhandener COM-Komponenten erhöhte Aufmerksamkeit erfordert.

Weiterhin können SOAP-Attachments wie E-Mails Viren enthalten. Zudem sollte ein Web Service Anhänge nur nach zusätzlicher Prüfung auf der Platte zwischenspeichern, um nicht unfreiwillig zum Upload-Dienst für einen Hacker zu werden. Schließlich sind Denial-Of-Service-Angriffe durch das Übertragen übergroßer Attachments denkbar.

Sicherungsmassnahmen

Bei Sicherungsmaßnahmen für webgestützte Anwendungen denkt man oft als erstes an SSL. Das ist wegen der Vertraulichkeit der in den SOAP-Parametern übertragenen Daten sicherlich ein richtiger Schritt. Jedoch ist vertrauliche Übertragung von Daten wenig wert, wenn der Empfänger nicht weiss, wer am anderen Ende sitzt. Deshalb sollte SSL-Verschlüsselung bei Web Services, die mit sensiblen Daten umgehen, immer mit einer Authentifzierung des Clients einher gehen. SSL-Client-Zertifikate oder eine Basic-Authentifzierung über HTTP lassen sich relativ einfach einsetzen, da sie transparent für den Web Service selbst sind.

Andererseits authentifiziert dies nur den SSL-Tunnel und nicht die durch ihn übertragenen SOAP-Nachricht. Sobald sie beim Web Service ankommt, ist der Absender nicht mehr sicher zu ermitteln.

Müssen Integrität und Authentizität der SOAP-Nachricht selbst gesichert sein, reicht SSL nicht aus. In diesem Fall kommen Zusatzstandards wie SAML ins Spiel.

Unabhängig von SSL ist die Prüfung der Parameter unerlässlich, da sogar eine authentifizierte und verschlüsselt übertragene SOAP-Nachricht manipulierte Werte enthalten kann.

Schließlich bildet nicht nur der Web Service, sondern auch die Infrastruktur, in der er läuft, ein mögliches Angriffsziel. Beispielsweise könnte ein Einbrecher Lücken in der SSL-Implementierung ausnutzen. Ein solcher Fehler kam bei OpenSSL vor einigen Monaten ans Licht.

Ein weiteres oft anzutreffendes Risiko ist die Sicherung des privaten SSL-Schlüssels des Webservers. Dieser liegt meist in einer Datei auf dem Filesystem, die prinzipiell zwar durch ein Passwort zu schützen wäre. Jedoch verzichten Administratoren oft darauf – sei es aus Bequemlichkeit oder weil sie den Server ohne Passwort-Abfrage starten wollen. Ohne diesen Schutz kann ein Dieb der Schlüsseldatei den Server „nachbauen". In Verbindung mit weiteren Angriffstechniken wie DNS-Spoofing vermag ein Client dann nicht mehr zwischen echtem und falschem Server zu unterscheiden. Am sichersten schützt davor die Aufbewahrung des privaten SSL-Schlüssels auf einer speziellen Hardware (HSM, Hardware Security Module). Fast alle derartigen Produkte bieten neben dem Schutz des privaten Schüssels eine Beschleunigung des SSL-Handshakes.

Da SSL kein Allheilmittel ist, muss man es durch weitere Massnahmen ergänzen. Dazu gehören Details bei der Implementierung des Dienstes und bei der Infrastruktur. Eine der einfachsten und gleichzeitig wirksamsten Massnahmen in der Web-Service-Implementierung ist eine sorgfältige Prüfung der in den Nachrichten übergebenen Parametern. Der erwähnte Angriff per SQL-Injektion ließe sich durch Kontrollieren der übergebenen Zeichenkette verhindern; etwa durch den Vergleich mit einem regulären Ausdruck. Auch die Länge der Parameterwerte sollte gegen ein sinnvolles Maximum geprüft werden.

Standards

Ersatz für die im eigentlichen SOAP fehlenden Sicherheitsmechanismen bieten ergänzende Standards, die meist spezielle SOAP-Header verwenden. So ist etwa die Identität des Absenders folgendermassen kodiert (s. Abb. 2):

- Die Identität des Benutzers wird digital signiert. Die Darstellung der Signatur in XML erfolgt dabei gemäß dem Standard XML-Signature.
- Ein in SAML definiertes XML-Element nimmt diese Identität auf.
- Seinerseits steht es in einem SOAP-Header, den WS-Security definiert.

Auf diese Weise können Web Services oder Proxies, die SAML unterstützen, eine SOAP-Nachricht mit einer gesicherten Absenderkennung versehen und diese verifizieren.

Die genannten Standards stellen zwar die Integrität auf Anwendungsebene sicher. Aber um sie verwenden zu können, müssen die Toolkits und Techniken, auf denen Web-Service-Client und -Server aufsetzen, sie unterstützen. In dieser Hinsicht unterscheiden sich SOAP-Toolkits noch stark. Weiterhin müssen die Implementierungen der Web Services zur Verwendung dieser Sicherheitsmechanismen (beispielsweise zur Erzeugung von SAML-Tokens) erweitert werden, was Entwicklungsaufwand erfordert und möglicherweise nicht gewünscht ist.

Den goldenen Mittelweg stellen spezielle SOAP-Filter oder Proxies dar, die transparent für die dahinterliegenden Web Services die sicherheitsbezogenen Aufgaben übernehmen. Das Spektrum reicht von der SSL-Terminierung mit Kontrolle der Client-Zertifikate über die Erzeugung und Prüfung von SAML-Headern bis hin zum Test der Parameterwerte. Auch administrativ kann solch eine Proxy-Lösung von Vorteil sein, da sie die Verwaltung der Sicherheitsfunktionen von der Anwendungsentwicklung entkoppelt, was gerade in großen Unternehmen wichtig ist.

Produkte

Obwohl Standards wie SAML noch recht jung sind, gibt es bereits etliche Produkte zur Sicherung und Filterung von SOAP-Nachrichten. Die folgende Aufzählung soll einen Eindruck davon geben, aus welchem breiten Spektrum sich die Anbieter in diesem Bereich rekrutieren.

Checkpoints Firewall-1 verfügt in der Version NG FP3 über eine einfache Möglichkeit, SOAP-Nachrichten anhand des Namespaces und des aufgerufenen Funktionsnamens zu filtern.

InterDo von Kavado ist eine Web-Application-Firewall, die Web-Anwendungen beispielsweise vor Angriffen wie Parameter- oder Cookie-Manipulationen schützt. In der neusten Version können bei diesem Produkt auch WSDL-Beschreibungen solcher Web Services hinterlegt werden, auf die der Zugriff über SOAP erlaubt sein soll. Zusätzlich prüft InterDo alle SOAP-Anfragen auf Konformität mit der WSDL-Beschreibung. Das stellt sicher, dass die in der Anfrage übergebenen Parametertypen mit der Schnittstelle des Web Services übereinstimmen.

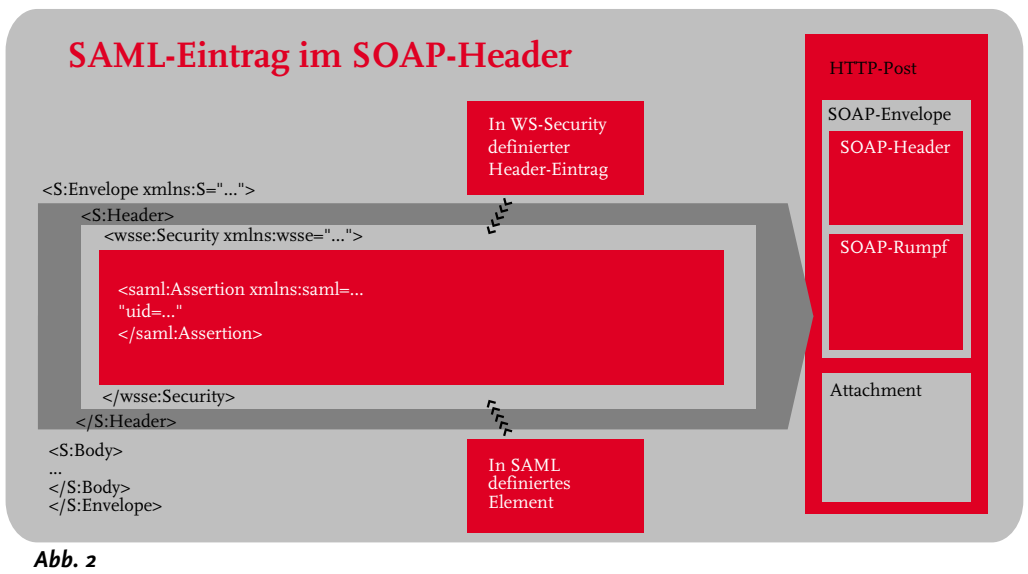


Abb. 2

Netegrity bietet mit dem TransactionMinder einen Zusatz für seine Web-Access- und Portallösung SiteMinder an. Es verwendet eine Benutzer-ID und die URL des Web Services als Kriterien für die Zugriffskontrolle. Erstere kann unter anderem aus einem SSL-Zertifikat, einem SAML-Header oder einem beliebigem Element der SOAP-Nachricht kommen. Ein besonderes Merkmal sind dynamisch ausgewertete Regeln, bei denen das Programm die Zugriffsentscheidung anhand der SOAP-Nachricht trifft (zum Beispiel Nachricht „Bestellung" nur akzeptieren, wenn Summe kleiner 10.000EUR).

Der SOAP Content Inspector (SCI) von Xtradyne stellt einen dedizierten Proxy zur Filterung von SOAP dar. Hinsichtlich Architektur und Bedienung ist das Produkt eng an einen schon länger vom Hersteller erhältlichen Proxy zur Zugriffskontrolle für CORBA-Anwendungen angelehnt. SCI vergibt die Zugriffsrechte anhand der ID und der Rolle des Benutzers sowie des angefragten Web Service, wobei die Rechte bis hin zu einzelnen Funktionen des Dienstes definiert werden können. Damit verfügt das Rechtemodell über eine sehr feine Granularität. SCI kann SAML-Header erzeugen und auswerten. Per XML-Schema lassen sich sogar gültige Wertebereiche für Parameter von SOAP-Nachrichten definieren.

Auch weitere zu SOAP-Filtern komplementäre Sicherheitsmassnahmen sind im Web-Service-Umfeld sinnvoll, beispielsweise sogenannte Secure Operating Systems. Dabei handelt es sich um Komponenten, die sich in das Betriebsystem einklinken und Systemaufrufe sowie Zugriffe auf Ressourcen (Dateien, Programme, oder auch Netzverbindungen) kontrollieren und Verstösse gegen die konfigurierte Policy blockieren.

Diese Systeme verhindern zwar nicht den Angriff selbst, können aber seine Folgen unterbinden. So könnte beispielsweise verhindert werden, dass ein erfolgreicher Einbrecher in den Webserver oder die Applikation per Buffer-Overflow eine Shell startet.

Fazit

Wichtig ist bei der Sicherheitskonzeption für einen Web Service immer, auch die gesamte Umgebung und alle Kommunikationsketten von Front- bis Backend zu berücksichtigen, da nur so ein angemessenes Gesamt-Sicherheitsniveau erreichbar ist.

Erschienen im Heise Verlag, iX 03/2003 – Stefan Middendorf ist Berater bei der cirosec GmbH und Mitautor des Buches „Java – Programmierhandbuch und Referenz für die Java-2-Plattform".

Stichtage für die IT-Branche 2003

Datum	Name der Veranstaltung	Veranstalter	Ort
12.06.03	Arbeitsrechtliche Aspekte der Internetnutzung am Arbeitsplatz	TÜV-Akademie	Berlin/DE
30.-31.07.03	Black Hat USA 2003 Briefings	Black Hat	Las Vegas/USA
04.-06.08.03	7th Annual IFIP WG 11.3 Working Conference on Data and Applications Security	IFIP	Estes Park/USA
02.-04.09.03	Information Security World Australasia 2003 Security World	Information	Melbourne/AUS
08.-10.09.03	6th International Symposium on the Recent Advances in IDS	RAID	Pittsburgh/USA
29.09.-02.10.03	Informatik 2003 - Teiltagung Sicherheit	GI	Frankfurt a.M./DE
07.-09.10.03	ISSE	EEMA, TeleTrusT	Vienna/AT
20.-24.10.03	Systems	Messe München	München
03.-05.11.03	The CSI 30th Annual Computer Security Conference	CSI	Washington,D.C./USA
20.-21.11.03	27. Datenschutzfachtagung - DAFTA	GDD	Köln/DE

Gastkommentar von Willi Kaczorowski

Die digitale Verwaltungsreform

Via Internet will der Bund die Verwaltung einfacher, effizienter und bürgerfreundlicher gestalten. In diesem Artikel wird beschrieben, welche Bedingungen der Online-Masterplan erfüllen muss.

Regelmäßig werden der öffentlichen Verwaltung fehlendes Kostenbewusstsein, mangelnde Kundenorientierung, verkrustete Strukturen und ein überdimensionierter Apparat vorgeworfen. Durch kleine Reformschritte müht sie sich, dem entgegenzuwirken; allerdings im Vergleich zur freien Wirtschaft regelmäßig mit einer Verspätung von fünf bis zehn Jahren. Die Verwaltung setzt nun mal keine Trends, sondern folgt ihnen. Deshalb ist auch die überfällige Strukturreform bisher ausgeblieben. Kein Berufsstand ist so abgesichert wie der öffentliche Dienst und hat dennoch so viel Angst vor Veränderungen. Daran hat sich noch jeder Innenminister die Zähne ausgebissen.

Unternehmen müssen sich ständig am Markt bewähren. Deshalb sind Unternehmen einem ständigen Wandel unterworfen, den die Beschäftigten im Grundsatz auch akzeptieren. Die öffentliche Verwaltung agiert unter anderen Rahmenbedingungen. Gemeinwohlorientierung, Rechtssicherheit, politische Verantwortlichkeit und Zuteilung ihrer Ressourcen prägen den Gestaltungsraum. Hinzu kommt ein Besoldungs- und Tarifrecht, das sich trotz kleiner Reformen immer noch eher am Dienstalter als am Leistungsprinzip orientiert.

Aufgrund der Globalisierung hat die Wirtschaft die Chancen zur Steigerung ihrer Produktivität und Kundenorientierung systematisch genutzt. Es wurden Bereiche geschlossen, Strukturen grundlegend auf den Kopf gestellt und den Beschäftigten gezielt geholfen, den neuen Herausforderungen standzuhalten. Dennoch wurde es in vielen Unternehmen ungemütlicher. Dies steht der öffentlichen Verwaltung noch bevor. Eine Verwaltung, die mehr leistet und weniger kostet, wie sie Innenminister Schily propagiert, ist ohne Strukturreformen nicht zu haben. Es gibt aber eine Chance, diese durchgreifende Veränderung der Strukturen und Abläufe zu erreichen. Sie ist mit dem Stichwort „electronic government“ charakterisiert.

Ziel ist es, mit Hilfe des Internets die Verwaltung einfacher, effizienter und damit kundenfreundlicher zu gestalten. Staatliche Dienstleistungen sollen rund um die Uhr abgerufen werden können. Künftig soll das gesamte Antragsverfahren von der Antragstellung bis zur Bezahlung über das Internet abzuwickeln sein. Vieles davon ist in Unternehmen heute schon eine Selbstverständlichkeit.

Wenn eGovernment vernünftig gemanagt wird, erhalten die Bürger öffentliche Leistungen schneller, qualitativ hochwertiger und kostengünstiger, und der Staat spart Geld. Im Masterplan eGovernment BundOnline 2005 geht allein der Bund von möglichen jährlichen Einsparungen von 400 Millionen Euro aus. Besonders die Reorganisation innerbehördlicher Dienstleistungen, beispielsweise des öffentlichen Beschaffungswesens, birgt ein erhebliches Potenzial.

So schön diese Perspektive für den Finanzminister ist: Geld wird nur gespart, wenn fünf Voraussetzungen erfüllt werden.

- Erstens: eGovernment muss auf Bundes-, Landes- und Kommunalebene miteinander verzahnt werden. Grundlage wäre ein Masterplan DeutschlandOnline 2005, der über die Initiative auf Bundesebene hinausgeht. Derzeit gleicht Deutschland einem Flickenteppich aus Einzellösungen und das kostet zusätzlich Geld. Wesentliche Geschäftsprozesse sollten über Behördengrenzen hinweg standardisiert werden.

- Zweitens: Deutschland wird ohne Rationalisierung der Kernverwaltung nicht auskommen. Nennenswerte Einsparungen können nur erzielt werden, wenn auch hier betriebsbedingte Kündigungen möglich sind. Die Umsetzung des eGovernment wird dazu führen, dass vor allem im kommunalen Bereich eine virtuelle Verwaltung entsteht. Call-Center-Technologie, Workflow-Einsatz, Wissensmanagement – all das ist nicht physisch an Standorte mit in Büros tätigen Beschäftigten gebunden. Einfache Antrags- und Genehmigungsverfahren eines Bürgers aus Hannover können auch durch Servicecenter in Berlin erbracht werden.

- Drittens: Für das neue Verständnis von öffentlicher Dienstleistung müssen die in der Kernverwaltung verbleibenden Beschäftigten sensibilisiert und geschult werden. Der Weiterbildung kommt ein hoher Stellenwert zu.

- Viertens: eGovernment-Dienstleistungen werden künftig auf Plattformen angeboten, die von Privatunternehmen betrieben werden. Für die Nutzung dieses Service können die Unternehmen im Auftrag des Staates eigene Gebühren erheben.

- Fünftens: eGovernment kann nur zu einer Modernisierung der Verwaltung beitragen, wenn es auch genutzt wird. Deshalb gehört der Ausbau der öffentlichen Internet-Infrastruktur zur Kernaufgabe der nächsten Jahre. Darüber hinaus werden Informationskampagnen und breit angelegte Schulungsprogramme durchgeführt werden müssen, damit Bürger und Wirtschaft die Vorteile einer digitalen Verwaltung auch erleben können.

Pressemeldung BSI 2003

Stefan Strobel, cirosec GmbH, Heilbronn

Security Outsourcing – Eine kritische Betrachtung

I. Einführung

Der Einsatz von Sicherheitssystemen wie Firewalls, Virenschutz-Gateways oder Intrusion Detection Systemen ist nichts Exotisches mehr. Entsprechend haben viele Organisationen die Anfangs-Euphorie hinter sich und kämpfen mit den täglichen Aufgaben beim Betrieb solcher Systeme. Wer zunächst glaubte, nur die Anschaffung einer Firewall wäre ein kostenintensives Vorhaben, der sieht sich heute mit einer Realität konfrontiert, in der die benötigten Software-Wartungsverträge sowie der Personal–aufwand für die ständige Aktualisierung, Konfiguration, Fehlerbehebung oder auch nur die Überwachung die ursprünglichen Anschaf–fungskosten langsam aber stetig überholen.

Outsourcing ist kein neues Thema und so ist es nicht verwunderlich, dass sich auch im Sicherheitsbereich viele Anbieter bemühen, den Firmen diese Arbeiten gegen monatliche Bezahlung abzunehmen. In den Jahren 2000 und 2001, als die Technologie-Börsen noch euphorisch gestimmt waren, galten Anbieter von „Managed Security Services“ als lohnende Investitionen. Viele Sicherheitsfirmen investierten Millionen in den Aufbau von gesicherten Rechenzentren („Secure Operating Centers“, kurz SOC) von denen aus sie die Firewalls ihrer Kunden überwachen und betreiben wollten. Seit dem Einbruch der Technologie-Börsen sind viele dieser Anbieter wieder verschwunden oder haben ihre Outsourcing-Angebote eingestellt. Einige haben bis jetzt überlebt und der Kunde findet eine ganze Reihe von verschiedenen, mehr oder weniger überzeugenden Angeboten.

II. Marktübersicht

Generell kann man die Angebote nach der Lage der Systeme und der Position des Personals unterscheiden. Die Grafik auf der nächsten Seite soll die Unterschiede darstellen.

Im ursprünglichen Fall ohne externe Unterstützung stehen die Systeme im Rechenzentrum der Organisation selbst und sie werden von eigenem Personal betrieben. Gelegentlich kommt es vor, dass die Konfiguration und Pflege einzelner Systeme externem Personal übertragen wird, wobei diese Personen nicht über Remote Access auf die Systeme zugreifen, sondern dauerhaft beim Kunden vor Ort beschäftigt sind. Vom Kunden werden die externen Mitarbeiter oft wie eigene Mitarbeiter in interne Abläufe eingebunden. Der große Unterschied ist nur, dass die Mitarbeiter nicht beim Kunden, sondern bei einem externen Dienstleistungsunternehmen angestellt sind. In der Regel ist dieses Modell teurer, als eigene Mitarbeiter einzustellen. Falls entsprechend qualifizierte Personen jedoch nicht am Arbeitsmarkt zu haben sind, ihre Ausbildung zu teuer wäre oder innerbetriebliche Politik die Einstellung weiterer eigener Mitarbeiter verhindert, kommen derartige Modelle zum Tragen. Es gibt sicher noch weitere Argumente, die für oder gegen eine solche, landläufig auch „Body-leasing“ genannte Konstellation sprechen. Für die Betrachtung von Managend Security und Security Outsourcing ist sie jedoch nicht besonders interessant und wird daher im Folgenden nicht weiter behandelt.

Eine andere, weniger interessante Variante: Das Unternehmen stellt die Geräte zu einem externen Anbieter, lässt den Betrieb und die Konfiguration jedoch beim internen Personal.

Der externe Anbieter übernimmt hier eigentlich nur den Anschluss an Strom und Netzwerk und die physikalische Zugangssicherung. Für IT-Sicherheitssysteme findet diese Variante nur selten Anwendung. Bei Webservern ist sie dagegen unter dem Namen Server Hosting oder Server Homing sehr verbreitet. Der Kunde profitiert dabei vor allem von einem kostengünstigen und gut ausgebauten Internet-Zugang des Anbieters. Interessant für Sicherheitsanwendungen sind vor allem Modelle, bei denen qualifiziertes externes Personal von einem sicheren externen Rechenzentrum (SOC) aus Überwachungs- und Wartungsaufgaben für den Kunden übernimmt. In diesem Segment findet man die meisten und vor allem die typischen Angebote wie „Managed-Firewall“ oder „Firewall-Monitoring“. Die Geräte selbst stehen dabei vorwiegend beim Kunden.

Beim „Firewall-Monitoring“ sind sowohl Personal als auch die Geräte bei einem externen Dienstleister zu finden. Ein typisches Beispiel ist ein „sicherer“ Internet-Anschluss, der schon beim Provider über eine Firewall und einen Virenscanner geht. Der Kunde nutzt damit eine zentrale Sicherheitsinfrastruktur des Providers gemeinsam mit anderen Kunden. Ähnlich verhält es sich bei externen Trustcentern, die digitale Zertifikate für Kunden ausstellen. Auch hier stehen die Geräte in einem sicheren Rechenzentrum des Anbieters und werden auch von ihm betrieben. Die Kunden bekommen nur das fertige Zertifikat zugestellt.

	Equipment intern	Equipment extern
Personal intern	Interner Betrieb oder „Bodyleasing“	selten sinnvoll, evt. Hosting
Personal extern (Fernwartung)	Firewalls/IDS Monitoring oder Management	Firewalls beim Provider, Scan oder Info-Service

Vergleich: Security-Management intern – extern

Eine Aufstellung über die Aufgaben beim Security-Outsourcing, eine nähere Betrachtung der einzelnen Angebote sowie eine abschließende Betrachtung und Zusammenfassung finden Sie bei www.cirosec.de unter Aktuelles/Veröffentlichungen.

„Apache Webserver“ und „Microsoft Internet Information Server“

Veröffentlichung der Sicherheitsstudien

Bonn, 2003 - Seit seiner „Erfindung“ Anfang der neunziger Jahre des letzten Jahrhunderts hat sich das World Wide Web (WWW) zu einem Medium entwickelt, ohne das die heutige Informationsgesellschaft kaum denkbar wäre. Die Informations- und Dienstleistungsangebote im WWW bilden eine Infrastruktur, die heute in vielen Bereichen nahezu unverzichtbar ist und deren Bedeutung in den nächsten Jahren eher noch zunehmen wird. Das Rückgrat dieser Infrastruktur bilden der Apache Webserver und der Microsoft Internet Information Server, die zusammen einen „Marktanteil“ von nahezu 90 Prozent erreichen.

Bei einem Webserver spielt das Thema Sicherheit eine besonders wichtige Rolle, da er naturgemäss eine sehr exponierte Position einnimmt. Dies wird von zahlreichen Sicherheitsvorfällen im Zusammenhang mit Schwachstellen in Webservern in den vergangenen Jahren illustriert, beispielsweise den Würmern CodeRed und Nimda, die sich im Jahr 2001 jeweils innerhalb kürzester Zeit im Internet verbreiteten und Millionen von Microsoft IIS Webservern infizierten. Auch der Marktführer Apache blieb von ähnlichen Problemen nicht verschont, allerdings erreichte beispielsweise Slapper im Sommer 2002 bei weitem nicht die Verbreitung von CodeRed und Nimda.

Das Bundesamt für Sicherheit in der Informationstechnik hat für die beiden „Marktführer“ Apache und IIS jeweils eine Sicherheitsstudie erstellen lassen. In diesen Studien wird die Architektur des jeweiligen Servers erläutert und es werden Hinweise für eine sichere Installation und Konfiguration sowie für einen sicheren Betrieb des jeweiligen Servers gegeben. Dabei wird auch die Konfiguration der zugrunde liegenden Betriebssysteme berücksichtigt.

Pressemeldung BSI 2003

Sicherheit im Zeitalter von E-Business macht ein strategisches Umdenken nötig

Einstürzende Mauern

Technische IT-Sicherheitskonzepte, die in den letzten zehn Jahren von Firmen implementiert wurden, haben sich vor allem auf die Absicherung der Netzwerkgrenzen konzentriert. Die enormen Kosten, die beim Aufbau und dem späteren Betrieb der komplexen DMZ-Strukturen entstehen und die gleichzeitig steigende Zahl von Verwundbarkeiten und erfolgreichen Angriffen, die von der klassischen Technik nicht verhindert werden können, machen ein strategisches Umdenken nötig.

Größere Firmen haben heute nicht selten so viele Firewalls, dass sie eine ganze Abteilung für ihren Betrieb benötigen. Sobald eine neue Anwendung oder eine neue Kommunikations-Anbindung zu einem Partner hinzukommt, werden bestehende Firewalls erweitert oder neue Firewalls aufgebaut. Betrachtet man die Regelwerke dieser Firewalls ein oder zwei Jahre nach ihrer Implementation, so stellt man fest, dass sie nahezu unüberschaubar geworden sind und eine Vielzahl von Regeln enthalten, die benötigte Protokolle für bestimmte Anwendungen freischalten. Diese Protokolle ermöglichen beispielsweise einem externen Anwender den Zugriff auf den öffentlichen Web-Server. Andere Regeln ermöglichen einer in Java, PHP, VB oder Perl geschriebenen Applikation auf dem Webserver den Zugriff auf eine interne SQL-Datenbank, um die aktuellen Lagerbestände, Lieferzeiten oder Produktbeschreibungen abzufragen und für die HTML-Anzeige aufzubereiten.

Auf diese Weise können externe Anwender über Web-Applikationen auf interne Systeme zugreifen. Dass dabei mehrere Firewalls, Server und Applikationssysteme hintereinander geschaltet sind, sieht der Anwender nicht. Dies ist auch so gewünscht. Der Anwender sollte nichts von der technischen Komplexität bemerken, selbst wenn zehn verschiedene Firewall-Systeme und Gateways in DMZs beteiligt sind, um Anfragen eines Anwenders zu internen Datenbanken oder Transaktionssystemen zu transportieren und die Ergebnisdaten aus den internen Systemen zum Anwender zurückzugeben.

Dies bedeutet aber auch, dass auch ein Hacker, der sich auf der Anwendungsebene bewegt, nichts von dieser komplexen Sicherheitsinfrastruktur bemerkt. Er bemerkt sie nicht und sie behindert ihn in keiner Weise bei seinen Angriffen auf Applikationsebene.

Löst man sich von den technischen Details solcher Angriffe, so erkennt man, dass man womöglich jahrelang versucht hat, sich mit Firewalls, Content-Security Produkten und ähnlichen Techniken einzumauern. Viele Organisationen haben vergeblich versucht, eine klare Grenze zwischen dem internen vertrauten Netz und der gefährlichen externen Welt zu ziehen. Je mehr der technische Fortschritt nach E-Business-Lösungen verlangt, umso mehr Anwendungen werden Partnern über eine Web-Schnittstelle angeboten und umso mehr Systeme bei Kunden und Lieferanten müssen möglichst direkt miteinander kommunizieren. Dabei wird sehr schnell deutlich, dass auch die dicksten mehrstufigen Firewalls immer mehr Löcher bekommen und dass das Ziel einer klaren Trennung zwischen Innen und Außen mit klassischer Sicherheitstechnik nicht erreichbar ist. Firmen, die versuchen alle extern erreichbaren Systeme in demilitarisierten Zonen aufzubauen, finden bald ihr gesamtes Rechenzentrum in DMZs wieder.

Die heutige Realität großer Firewall Systeme sind meist Strukturen, die an vielen Stellen durchlöchert sind und bei denen die Dicke der Mauer keinen Einfluss auf die Größe der Löcher besitzt.

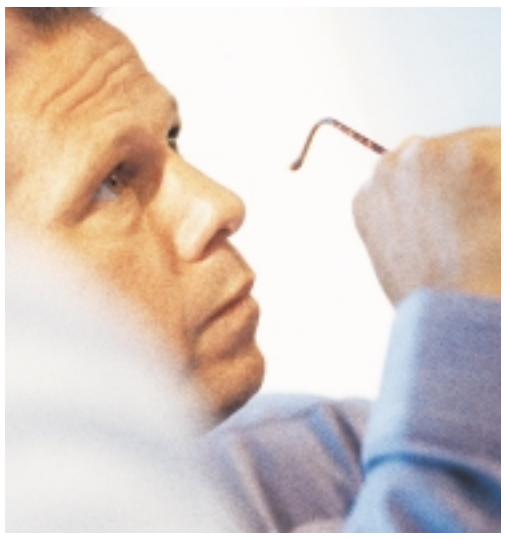
Die Konsequenz aus dieser Problematik ist natürlich nicht, dass Firewalls keinen Sinn mehr haben oder sogar abgeschafft werden sollten. Man sollte sich jedoch bewusst sein, dass sie kein Allheilmittel sind und dass es keinen Sinn macht, beliebig viele Firewalls hintereinender aufzureihen, um die Sicherheit zu erhöhen. Stattdessen sollte man sich für neue Sicherheitstechniken interessieren, die einen effektiven Schutz auf Anwendungsebene ermöglichen. Die Produkte in diesem Umfeld sind zahlreich, jedoch in Deutschland noch nicht so verbreitet wie beispielsweise in den Vereinigten Staaten, obwohl viele Produkte bereits seit drei Jahren oder noch länger auf dem Markt sind.

Stefan Strobel,
Geschäftsführer der cirosec GmbH
und Autor des Buches „Firewalls und IT-Sicherheit“

Investitionschancen für IT-Unternehmen in Deutschland

E-Business nach der Euphorie

Die Informations- und Kommunikationstechnologien verändern die inner- und zwischenbetrieblichen Prozesse in allen Zweigen der Wirtschaft tiefgreifend. Nach der ersten Euphorie wird in den Unternehmen das Potenzial von E-Business zur Optimierung aller Prozesse inzwischen nüchterner hinsichtlich seiner Effizienz hinterfragt.



Im Zusammenhang mit der Herausgabe des E-Business-Jahrbuchs der deutschen Wirtschaft führten deshalb der Bundesverband der Deutschen Industrie e. V. (BDI) und der Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e. V. (BITKOM) im Zeitraum Feb. - März/April 2003 eine Befragung bei über 10.000 Industrie- und Dienstleistungsunternehmen in der deutschen Wirtschaft durch. Ziel der Befragung, die durch das Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) und der Wegweiser GmbH Berlin betreut wurde, ist es, konkrete Aussagen über den zukünftigen Einsatz von eBusiness entlang der gesamten Wertschöpfungskette in deutschen Unternehmen zu erhalten.

Themenschwerpunkte der Befragung sind:

- Bedeutung von E-Business in Unternehmen und Branchen 2003 - 2004
- Analyse bereitgestellter Finanzmittel, Personalressourcen und Mitarbeiterqualifikation für die Umsetzung von E-Business und Eruierung von Hemmnissen
- Bedeutung von Standards im zwischenbetrieblichen Geschäftsverkehr
- Realisationsstand von E-Business, Investitionsabsichten und Stand der Umsetzung
- Tendenz der Investitionsentwicklung für Beratungsleistungen, Standardsoftware, Entwicklungs- und Integrationsdienstleistungen, Individualsoftware sowie IT-Hardware
- Erwartungen an E-Business („return on investment“) sowie eine Evaluation von Entscheiderstrukturen in Unternehmen

Der Forschungsansatz „Multi Client“ ermöglicht einer beschränkten Anzahl von Unternehmen sich am Projekt „eBusiness-Konjunktur-Barometer“ mit eigenen Fragestellungen zu beteiligen. Erste Ergebnisse eines Pre-Tests anlässlich der „Stuttgarter eBusiness-Tage 2002“ zeigen, dass die Tendenz der Investitionsentwicklungen im IT und eBusiness wieder leicht ansteigt. 46 Prozent der Teilnehmer erwarten zunehmende Investitionen im zweiten Halbjahr 2003 verglichen mit dem 2. Halbjahr 2002, weniger als 7 Prozent rechnen mit eher abnehmenden Investitionen, die restliche Anzahl geht von einem gleichbleibenden Niveau aus. Nur 8 Prozent der Unternehmen gaben an, dass E-Business-Anwendungen bereits vollständig umgesetzt seien. Im Bereich der Bereitstellung von IT-Infrastrukturen für E-Business besteht bei 87 Prozent der Unternehmen noch Handlungsbedarf.

Die vollständigen Ergebnisse der Befragung werden im E-Business-Jahrbuch der deutschen Wirtschaft (print und online) zusammenfassend dargestellt. Daneben enthält das Jahrbuch einen umfassenden Marktüberblick über Produkte und Dienstleistungen für die Abbildung elektronischer Geschäftsprozesse.

„Das eBusiness-Jahrbuch der deutschen Wirtschaft wird dabei helfen, den Markt transparenter zu machen. Anbieter und Nachfrager entsprechender Lösungen finden leichter zusammen. Zudem vermittelt es wichtige Informationen über die heutige Nutzung der neuen Medien in der Industrie und über die dort verwendeten Standards“, so Dr. Michael Rogowski, Präsident des Bundesverbandes der Deutschen Industrie e.V.

Pressemeldung BSI 2003

IT-Defense 2004 – Der IT-Security-Kongress, u.a. mit Capt´n Crunch

Bruce Schneier hat seine Teilnahme zugesagt

HEILBRONN, Juni 2003 – Wie in diesem Jahr wird die IT-Defense auch 2004 an einem ganz besonderen Ort stattfinden. Die Veranstalter haben für die IT-Defense die ehemalige Garnisonsbäckerei in Ludwigsburg ausgewählt. Dort, wo 1871 noch die königlichen Brötchen gebacken wurden, werden 2004 Branchengrößen aus Europa und den USA die neusten Trends der IT-Sicherheit diskutieren.

Die ehemalige Garnisonsbäckerei in Ludwigsburg in der Nähe von Stuttgart besticht nicht nur durch die historische Fassade dieses denkmalgeschützten und komplett sanierten Backsteinbaus. Auch die unmittelbare Nähe zum prachtvollen Residenzschloss prägen Stil und Lage des nestor Hotels.

150 vollklimatisierte Zimmer und Suiten mit bester Ausstattung warten auf die Teilnehmer.

Auch das Programm verspricht wieder sehr interessant zu werden. Die Veranstalter konnten schon einige renommierte Referenten gewinnen. Neben Bruce Schneier hat auch James Bamford bereits zugesagt. Lance Spitzner wird über Honeynets referieren und Aaron Newman zum Thema „Sicherheit von Oracle Datenbanken“. Auch konnte die Hacking-Legende Capt'n Crunch für die IT-Defense 2004 gewonnen werden.

Bruce Schneier ist ein international anerkannter IT-Sicherheitsexperte, Buchautor und Gründer von Counterpane Internet Security, Inc..

Bruce Schneier

Seine bekanntesten Bücher sind „Secrets & Lies: Digital Security in a Networked World“ und „Applied Cryptography“. Daneben ist er Autor des freien E-Mail-Newsletters „Crypto-Gram“. Er entwickelte den populären Blowfish-Verschlüsselungs-Algorithmus und war mit Twofish Finalist für den Federal Advanced Encryption Standard (AES).

James Bamford ist Autor der Bücher „The Puzzle Palace“ und „Body of Secrets“, die beide internationale Bestseller sind. Sein jüngstes Buch „Body of Secrets“ handelt von den Machenschaften der NSA. In diesem Buch nimmt er Bezug auf die Sicherheitsverletzungen der NSA im Vorfeld der Anschläge vom 11. September 2001 und führt den Leser in das Innerste der amerikanischen Spionagewelt.

Der legendäre Hacker Captain Crunch ist einer der bekanntesten Hacker im digitalen „Untergrund“. Mittlerweile kann er mehr als 30 Jahre Erfahrung im Bereich der Programmierung und der Security vorweisen. Er machte sich 1971 einen Namen, als er entdeckte, dass die Spielzeugpfeife in der Capt'n Crunch-Cornflakes Box dazu verwendet werden konnte, kostenlos zu telefonieren. Daneben hat er das erste Textverarbeitungsprogramm überhaupt entwikkelt, das 1981 mit dem ersten IBM PC auf den Markt kam.

Als Sicherheitsexperte für Datenbanken ist Aaron Newman weltweit bekannt. Er ist Co-Autor des Oracle Security Handbook und hat mehrere Whitepapers zu diesem Thema geschrieben.

Lance Spitzner hat sich der Erforschung von Honeynet-Technologien und deren Nutzung verschrieben, um mehr über den Feind – die Bad Guys – zu lernen. Er ist Gründer des Honeynet Projektes, Moderator der Honeypot Mailing-Liste, Autor von „Honeypots: Tracking Hackers“, Co-Autor von „Know your Enemy“ und Autor einiger Whitepapers.

Aktuelle Informationen unter: www.it-defense.de

kommentare

Kommentare der Referenten zur IT-Defense 2003:

Bill Cheswick
I always enjoy coming to your conferences. I run into a different set of speakers than those usually touring in the States, and it is good to hear what the others are up to. The attendees tend to be unusually well-informed, and I always come home with some new ideas and insights.

Simple Nomad
Not only was this a good conference for me as a presenter, between the conversations with the other speakers and the attendees themselves I came away with new ideas for future research projects. That was a surprise, and is an excellent indication of the value of the conference for me.

Simon Singh
IT-Defense provides an excellent forum for exchanging the latest ideas in what is a fast changing and challenging topic. It is an excellent opportunity to gather some of the most respected experts in the world, from diverse backgrounds and in an environment that is both informal and intimate.

Gerald Brose
An dieser Stelle erstmal herzlichen Glückwunsch zu Ihrer rundum gelungen Veranstaltung, die mir viel Spaß gemacht hat. Ich fand das Programm sehr interessant und wäre gerne noch am Donnerstag und Freitag dageblieben. Sowohl die Wahl des Veranstaltungsortes wie die Auswahl der Redner waren klasse, die Organisation wirklich perfekt. Also ein dickes Lob!

Hans-Jürgen Stenger
In den beiden Tagen habe ich mehr gelernt als bei einem anderen Seminar mit vergleichbarem Thema, das über 14 Tage ging. Nochmals vielen Dank bei dieser Gelegenheit, dass Sie seine Teilnahme ermöglicht haben.

Die IT-Zeitung der cirosec GmbH und des dpunkt. Verlages

Mediadaten 2003/04

Format	DIN A3, 297 x 420 mm
Umfang	8 Seiten
Papier	70 g/qm, Zeitungsdruck
Druck	4/4-farbig
Farbskala	Euro-Skala
Druckverfahren	Offset
Druckvorlagen	60er Raster
Erscheinungsweise	2 x jährlich
Verteilung	**(3.000 Stück)** (Direkt-) Versand für Banken, Versicherungen, Institutionen, Handel und Industrie
Verteilungsgebiet	Deutschland
Redaktion	cirosec GmbH, dpunkt.verlag, MuKK
Anzeigenvertrieb	cirosec GmbH Ferdinand-Braun-Str. 3 74074 Heilbronn Telefon: 07131 - 59455-0 Telefax: 07131 -59455-99 E-Mail: info@cirosec.de dpunkt.verlag GmbH Ringstraße 19B 69115 Heidelberg Telefon: 06221-14830 Telefax: 06221-148399 E-Mail: hallo@dpunkt.de
Gesamtproduktion Satz und Layout	MuKK, Marketing und Kommunikationsdesign Konstanz Nordstr 28 • 74076 Heilbronn Telefon: 07131 - 911 854 Telefax: 07131 - 911 853 ISDN: 07131 - 486 610 (Leonardo, Mac) E-Mail: info@mukk-hn.de