

Contents

1. Editorial
2. Neuerungen der scip AG
3. Neue Sicherheitslücken
4. Technischer Fachartikel
5. Linktipps
6. Software-Tipps
7. Buchtipps
8. Multimedia
9. Kreuzworträtsel
10. Literaturverzeichnis
11. Impressum

1. Editorial

IT-Security Standards: Segen und Fluch

Da Sie den scip monthly Security Summary abonniert haben, gehe ich davon aus, dass Sie sich gezielt und tiefergehend mit IT-Security auseinandersetzen.

Ist Ihnen in den letzten Monaten aufgefallen, wovon am meisten, abgesehen von den unzähligen

Wurmmeldungen, berichtet wurde? IT-Security

Standards. Da werden Abkürzungen und Begriffe feilgeboten: ISO 17799, BS 7799-1, BS 7799-2, BSI, CC, ITSec, Orange Book, Grundschutzhandbuch, Basel II, EU-Framework Decision 2002, Österreichisches IT-Sicherheitshandbuch, KonTraG, TDDSG, CH-Datenschutzgesetz uvm.

Was ist das Ziel eines Standards? Schon hier scheiden sich die Geister. Für die einen müssen



Kennzahlen her, um strategische Entscheide zu fällen, andere möchten einen Leitfaden für Ihre Auditoren, noch andere verlangen die Erhöhung der Sicherheit usw. Gemäss Duden wird Standard wie folgt definiert: Massstab, Richtschnur, Norm; Qualitäts- oder Leistungsniveau. Es wird nicht darauf hingewiesen, dass durch einen Standard effizienter oder kostengünstiger gearbeitet wird. Ebenso steht nirgends, dass die anfallenden Aufgaben vereinfacht werden. In einer Zeit, in der es in der IT vermehrt um Effizienzsteigerung und Optimierung der bestehenden Infrastruktur geht, sehr erstaunlich.

Ich für meinen Teil habe meine eigenen Erfahrungen mit der Umsetzung von ISO Standards gemacht. Zudem habe ich vor einigen Jahren das BSI IT-Grundschutzhandbuch erworben und mich damit befasst. Da OpenSource im Bezug auf IT-Security einige Vorteile aufweist, habe ich mich auch mit dem Open Source Security Testing Methodology Manual (OSSTMM) auseinander gesetzt.

Seit längerem verfolge ich ein Ziel und bin fest davon überzeugt, dass es **nachvollzieh- und umsetzbare Standards innerhalb der IT-Security benötigt**. Nur so sind Ergebnisse aussagekräftig, vergleichbar, greifbar sowie Investitionsüberwachungen und Zielkontrollen einführbar, anpassbar und durchführbar.

Umfassende Standards ergeben Mehraufwand.

Sei dies in der Anpassung der Umgebung an die Richtschnur, der täglichen

Auseinandersetzung der Mitarbeiter sowie der extra dafür eingesetzten internen und externen Spezialisten damit. Da Standards (ansich) nicht die Arbeit erleichtern, werden sie in den

meisten Fällen als notwendiges Übel betrachtet und so gut wie möglich umgangen. Aus der Physik ist uns bekannt, dass alles versucht in eine Position zu gelangen in welcher es am wenigsten Energie aufwenden muss. So auch wir

Menschen.

Verstehen Sie mich nicht falsch, wir bedürfen Standards. Aus meiner Erfahrung weiss ich aber auch, dass Standards auf den ersten Blick gut aussehen, bei der täglichen Arbeit aber für viele Fragen und Subprozesse verantwortlich zeigen. Desweiteren sind Standards nicht das Allheilmittel der IT-Security Branche. Heutzutage wird in Securitykreisen darauf verwiesen, dass man die letzten Jahre falsch gearbeitet hat und daher viele Fehler begangen wurden (z.B. unbrauchbare IDS-Integrationen). Diese Fehler mache man aber jetzt nicht mehr, man hat ja einen Standard.

Haben wir den wirklich? Und wofür genau haben wir einen Standard? Nach einigen interessanten Gesprächen mit Personen aus dem IT-Security-Umfeld, von Finanzinstituten, Herstellern, Industrie und Konkurrenz, ist bei mir diese Aussage hängengeblieben: „Die (IT-Securityanbieter) machen das selbe wie vor 5 Jahren, nur sagen sie nicht Produkt A und B lösen Ihre Probleme, sondern durch die Umsetzung von Standard G werden Ihre Probleme gelöst.“ Eine IT-Security Kultur [scip AG 2003a] wird leider noch immer vermisst.

Dabei begeht man die selben Fehler vor denen man die Kunden, gemäss Marketing, schützen möchte. **Eine inkonsequente oder gar nicht durchgeführte Bedürfnisanalyse und Zieldefinition.**

Kundenorientiertheit beginnt bei der Frage: „Was benötigt der Kunde und was nützt dem Kunden.“ Ein Standard kann keine Probleme lösen. Dafür ist er zu gross, unflexibel, statisch und zu oberflächlich. Zudem bringt diese Grossinvestition, bei den meisten Firmen, keinen finanziellen Gewinn, schon gar nicht direkt. So lange keine klaren Richtlinien (Gesetzte) von statlicher Seite definiert sind, nach welchen sich die Firmen richten müssen (analog der Buchhaltung für AG's), werden, verständlicherweise, nur vereinzelte Firmen einen solchen Kraftakt umsetzen. Für und bei Finanzinstituten sind ja diesbezüglich schon verschiedenste Regeln in Kraft, welche durch die Informations Technologie zwingend umgesetzt werden müssen.

Damit ist das Problem aber nicht vom Tisch. Zur Rückverfolgbarkeit, Diskutierbarkeit und Nachprüfung von Ergebnissen braucht es Vorgaben. Unserer Meinung nach sind dedizierte Standards (lokalisierte Standards), dem Kunden angepasst und doch auf einen globalen Standard basierend sowie die Übergabepunkte der

scip monthly Security Summary
Marc Ruef & Simon Zumstein
scip_mss-19_10_2003-1.doc

errechneten Werte definiert, ein dem Kunden die notwendige Transparenz schaffender und dadurch nützlicher Dienst.

Falls Sie dennoch die zu Beginn erwähnten Methoden in einen Kontext stellen möchten, hier eine kleine Einordnung, vielen Dank an Herrn Fey (IT-Audit.de):

Es gibt Audits / Zertifizierungen / Testate in Richtung ISO 17799 (Sicherheitsmanagement), ISO 9000 ff. (Qualität), ITIL (Steuerung des IT-Betriebs), COBIT (Steuerung der IT), EISA-Methode (Sicherheit) oder nach dem BSI IT-Grundschutzhandbuch (Sicherheit).

Simon Zumstein <sizu@scip.ch>
Zürich, 16. Oktober 2003

2. Neuerungen der scip AG

2.1 Lizenzmanagement

Heutige Sicherheitsinfrastrukturen übernehmen mannigfaltige Aufgaben. Absicherung der Zonen, Spamschutz, Content Scanning, Firewalling, Intrusion Detection, Host-Sicherheit usw. Diese Aufgaben werden durch unterschiedliche Systeme und Softwares bewerkstelligt.

Zur Sicherstellung der Aktualität der eingesetzten Softwares oder zur Minimierung der Ausfallzeit wurden Depotwartungen, Softwarewartungen und Gold-States erworben. Diese müssen jedes Jahr erneuert werden.



The screenshot shows the SCIP website interface. At the top, there is a navigation bar with the company name and contact information. Below that, a red banner displays a security alert: "15.10.2003 Microsoft Windows Messenger Service Bufferoverflow". The main content area features a heading "Herzlich willkommen bei der scip AG" followed by a paragraph about the importance of security in the current context. Below this, a table lists services under three categories: CONSULTING, INFORMATION, and PROCESS. At the bottom, there is a footer with the company's mission statement and contact details.

CONSULTING	INFORMATION	PROCESS
Security Assessment	ipallas! Informationsdienst	Projektmanagement
Penetration Testing	Emergency-SMS/ Mobilelösung	Methodiken aus Erfahrung
Security Audit	adchileus! direkter Datenfeed	Prototyping
Betriebsconsulting	Vorfertbarkeits-Datenbank	Lizenzmanagement
Security Reviews	scip monthly Security Summary	Proof of Concept
Vulnerability Assessment	Fachartikel in Zeitschriften	Service Level Agreement
Security Awareness	Publikationen	Datenbanken
Firewallpolicy Assessment	Merkbücher	Workshops
	scip Security Ticker	

Sicherheitsarchitekturen:
VPN, Firewalling, Intrusion Detection, Intrusion Prevention, Log-Management, E-Mail Verschlüsselung, Vulnerability Management, PKI, Client/Server Security, Hochverfügbarkeit, Entry Infrastrukturen, Content Scanning, Virenschutz usw.

Konzept, Assessment, Architektur, Realisierung, Workshop, Fachreferat

Die meisten dieser abgeschlossenen Verträge haben nicht die selbe Laufzeit, Begrenzung, Kündigungstermine geschweige denn Leistungsumfang. Jeder Hersteller oder gar Wiederverkäufer definiert seine eigenen Spielregeln. Nur wenige erlauben die Synchronisation der Laufzeiten auf das

News, Webseite, Security, Sicherheit
public
Seite 2/16

Die Software muss nicht installiert werden und benötigt im Hintergrundbetrieb nur 0,1 MByte RAM. Dabei senden Sie keinerlei Daten an uns. Es werden lediglich die neusten Informationen ab unserer Website heruntergeladen. Der Zyklus der Downloads lässt sich manuell den eigenen Bedürfnissen anpassen.

Das Tool ist in der Version 1.05 als Ticker definiert. Obwohl es in der Lage ist besonders wichtige oder teilweise Ihr System betreffende Sicherheitslücken hervorzuheben (z.B. Schwachstellen im Microsoft Internet Explorer).

2.4 Neue Schulungen

Anhand der Anfragen bezüglich spezifischer Vertiefungslehrgänge hat sich die scip AG dazu entschlossen zusätzliche Schulungen zu entwickeln. Diese sprechen gezielt Security Engineers und Techniker an. Das Credo der neuen Workshops ist das vermitteln von Hintergrundwissen zu spezifischen Bereichen der IT-Sicherheit.

Momentan werden diese beiden neuen Schulungen angeboten:

- Virologie (Computerviren, Trojaner und Hintertüren)
- Attacken (Denial of Service-Attacken, Bufferoverflow, Cross Site Scripting, Race-Condition, Evasion uvm.)

In der Ausarbeitung befinden sich noch die Themen: Intrusion Prevention und Log-Management.

Sie finden diese und weitere Workshops auf unserer Website <http://www.scip.ch>.

AG (Marc Ruef) verfassten Artikel „Intrusion Detection - Mit Linux Angriffe erkennen und analysieren“ [Ruef 2003].

Das Inhaltsverzeichnis der aktuellen Ausgabe des LinuxEnterprise Magazins finden Sie unter <http://www.linuxenterprise.de/itr/ausgaben/psecom,id,166,nodeid,16.html>.

2.6 Workshopinweise

Oktober 2003	
22.10.2003	Log Management [LMFT]
23.10.2003	IDS / Intrusion Prevention [IDRT]
24.10.2003	Virologie [VLVE]
November 2003	
04.11.2003	Profiling [PRPT]
07.11.2003	Virologie [VLVE]
14.11.2003	Attacken [ATVE]
17.11.2003	Intrusion Prevention [IPVE]
18.11.2003	Viren [VIFT]
21.11.2003	Virologie [VLVE]
22.11.2003	scip Security Process [sSP]
26.11.2003	Vulnerability Assessment [VUST]
27.11.2003	Log Management [LMST]
28.11.2003	Attacken [ATVE]

Das scip AG Workshop-Portfolio finden Sie auf der Firmenwebseite <http://www.scip.ch>.

Seminarbezeichnung	Code	Dauer	Datum	Preis (CHF)	Status	Anmelden
Viren	VIFT08	16-18 Uhr	18.11.2003	150.-	Offen	Anmelden
IDS / Intrusion Prevention	IDRT03	16-18 Uhr	19.11.2003	150.-	Offen	Anmelden
scip Security Process	sSP008	09-13 Uhr	22.11.2003	190.-	Offen	Anmelden
Seminarbezeichnung	Code	Dauer	Datum	Preis (CHF)	Status	Anmelden
Log Management	LMFT04	09-13 Uhr	07.11.2003	500.-	Offen	Anmelden
Seminarbezeichnung	Code	Dauer	Datum	Preis (CHF)	Status	Anmelden
Profiling	PRPT08	09-17 Uhr	04.11.2003	850.-	Offen	Anmelden
Seminarbezeichnung	Code	Dauer	Datum	Preis (CHF)	Status	Anmelden
Virologie	VLVE02	08-16 Uhr	07.11.2003	1450.-	Offen	Anmelden
Attacken	ATVE02	08-16 Uhr	14.11.2003	1450.-	Offen	Anmelden
Intrusion Prevention	IPVE01	08-17 Uhr	17.11.2003	1450.-	Offen	Anmelden
Virologie	VLVE03	08-16 Uhr	21.11.2003	1450.-	Offen	Anmelden
Attacken	ATVE03	08-16 Uhr	28.11.2003	1450.-	Offen	Anmelden

2.5 Fachartikel der scip AG

In der aktuellsten Ausgabe des Linux Enterprise Magazin 11.2003, finden Sie einen durch die scip

scip monthly Security Summary
 Marc Ruef & Simon Zumstein
 scip_mss-19_10_2003-1.doc

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.

Die Dienstleistungspakete [\)scip\(pallas](#) liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.

Contents:

- 3.1 Microsoft Windows Messenger Service Pufferüberlauf
- 3.2 Microsoft Windows RPC Race Condition Denial of Service

3.1 Microsoft Windows Messenger Service Pufferüberlauf

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 15.10.2003
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=332>

Der "Messenger Service" ist nicht mit dem eigenständigen Produkt Microsoft MSN Messenger zu verwechseln. Der hiervon betroffene "Messenger Service" ist per Default auf den Betriebssystemen Windows NT, 2000 und XP - Server und Workstation Version, aktiviert. Dieser Pufferüberlauf kann es einem Angreifer ermöglichen, willkürlich, beliebigen Code auf dem betroffenen System auszuführen. Dies mit Administrations-Privilegien. Der befallene "Messenger Service" ist zuständig für die bekannten Pop-Ups. Es können die unterschiedlichsten Meldungen auf den Bildschirm der vernetzten Computer angezeigt werden (z.B. Server wird in 10 Minuten heruntergefahren, bitte ausloggen). Dieses Feature ist nicht wirklich Business kritisch und kann einfach deaktiviert werden. Der "Messenger Service" kann auch via Microsoft RPC angesprochen werden. Dies ist jedoch nicht mit dem im z.B. W32.Blaster ausgenutzten RPC-DCOM zu vergleichen. DCOM ist ein objektorientierter Mechanismus welcher von den unterschiedlichsten Microsoft Programmen angesprochen werden kann (z.B. Microsoft Exchange). Da der "Messenger Service" via RPC aufgerufen werden kann wird darüber spekuliert ob er auch über SMB (Server Message Block) lauffähig ist.

Expertenmeinung:

Ein in den meisten Fällen gar nicht benutztes Feature, ist Ausgangslage für eine weltweite

Patcherei. Da beinahe alle Windowssysteme betroffen sind, wird schnell ein Exploit zu dieser Schwachstelle in den Umlauf gelangen. Die Auswirkungen solcher Exploits sind uns mehr als bekannt (SQL Slammer, W32.Blaster). Da diese Schwachstelle über UDP Anfragen ausgelöst werden kann, wird sich ein allfälliger Wurm in windeseile verbreiten. Wie immer sind jene gut bedient, welche mehrstufige Sicherheitsvorkehrungen getroffen haben, wie z.B. Zonenkonzeption, Hardening, Netzunterteilung und Abschottung, ACL, MAC usw.. Trotzdem werde auch diese Systeme in Netzen betrieben, welche von unterschiedlichen Gruppen ansprechbar sein müssen. Es gilt den Patch umgehende zu applizieren. Bei "internen" Angreifern sind ausgedehntere Massnahmen zu treffen.

3.2 Microsoft Windows RPC Race Condition Denial of Service

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 14.10.2003
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=331>

Durch die Ausnützung dieser Microsoft RPC Schwachstelle ist es einem externen Angreifer möglich, den RPC-Dienst zu killen, das System unansprechbar oder gar zum Absturz zu bringen. Von dieser Verletzbarkeit sind beinahe alle Systeme betroffen. Inklusiv der mit dem Microsoft Security Bulletin MS03-039 gepachten Systeme (<http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=277>). Es wird nicht die selbe Schwachstelle ausgenutzt welche im Bulletin MS03-039 beschrieben wird. Diese Verletzbarkeit kommt aufgrund einer fehlerhaften Abarbeitung von mehreren aneinander gereiten RPC Anfragen zustande. Durch das ausnützen der nicht optimalen Verarbeitung dieser zeitkritischen und von einander abhängigen Prozesse kann das System in die Knie gezwungen werden. Bis jetzt wurde nicht nachgewiesen, dass durch das ausnützen dieser Schwachstelle beliebiger Code auf dem angegriffenen System ausgeführt werden kann.

Expertenmeinung:

Wieder einmal ist der zur Berühmtheit gelangte RPC-Dienst (Bsp. W32.Blaster [<http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=178>]) der Microsoft Windows Systeme betroffen. Der sehr komplexe RPC-Dienst bietet anscheinend einige Angriffsflächen. Es wird davon ausgegangen, dass Microsoft wieder einen Patch zur Verfügung stellen wird. Es bleibt jedoch fraglich ob nicht die

Integration des RPC Dienstes selbst angepasst werden muss (falls ökonomisch machbar) oder per Default zusätzliche Sicherheitsmechanismen angewandt werden sollten. Eine mehrschichtige Sicherheitskonzeption kann dabei behilflich sein.

4. Technischer Fachartikel

4.1 Auditing mit Linux – Teil 2: Entdecken Sie die Schwachstellen Ihres Systems

Erkennen der Server-Anwendung

Konnten Ports als offen und ansprechbar identifiziert werden, gilt es den angebotenen Dienst zu identifizieren. Die IANA gibt periodisch eine Liste heraus, die als Empfehlung für die Vergabe der Portnummern angesehen wird. So sollte sich nach dieser Portliste auf dem Port 23 der TELNET-Dienst finden. Port 25 ist für SMTP (Simple Mail Transfer Protocol, RFC 821) und Port 80 für HTTP (Hypertext Transfer Protocol) vorgesehen. Wir können also anhand der Ausgabe des Portscanners vermuten, um was für einen Dienst es sich handelt.

Diese Liste ist jedoch nur eine Empfehlung. Genauso wie bei den RFCs haben sich weder die Administratoren noch die Entwickler oder Anwender an diese Vorgaben zu halten. So ist es nicht selten gesehen, dass ebenso auf dem TCP-Port 81 ein HTTP-Dienst angeboten wird. Zum Beispiel, um mit dem gleichen Hostnamen auf einem anderen Port ein anderes Webangebot bereitzustellen. Oder oft finden sich auch auf diesen Ports Administrations-Schnittstellen für irgendwelche Dienste. Ähnliches ist auf den Ports 82, 800 und 888 zu beobachten.

Die Gruppe THC (The Hackers Choice) brachte eine Anwendung namens amap (Application Mapper) - in Anlehnung an das populäre Scanning- und Auswertungstool nmap von Fyodor - heraus. Diese baut eine Verbindung zu einem oder mehreren Zielpoints auf, schickt irgendwelche Anfragen und versucht anhand der Rückgaben das eingesetzte Protokoll zu erkennen. Dies ist sehr gut für automatisierte Prozesse, bei denen man mehrere Hosts und Ports überprüfen sollte.

```
maru@debian~$ amap -s T www.scip.ch 80
Total amount of tasks to perform: 11
Amap v0.95 started at Thu Jul 3 11:25:05
2003, stand back and keep the children away.
Protocol on IP 192.168.0.2 port 80 tcp mat-
ches HTTP
Unidentified ports: None.
Amap v0.95 ended at Thu Jul 3 11:25:10 2003
```

Möchte man diese Überprüfung manuell durchführen, kann man sich einer Terminal-Emulation, wie zum Beispiel TELNET oder Net-Cat, bedienen. Sodann baut man eine Verbindung zu einem ansprechbaren Port auf und setzt irgendwelche Anfragen ab. Kennt man sich mit

den verschiedenen Protokollen der Anwendungsschicht genug gut aus, kann man anhand des Verhaltens und der Rückgabe des Servers das angebotene Protokoll erkennen. Man macht schlussendlich genau das gleiche, was auch amap macht. Wie man mit den jeweiligen Servern zu sprechen hat, liest man am besten in den jeweiligen RFCs nach.

Identifizieren der Server-Implementierung

Die meisten interaktiven Netzwerkanwendungen der Anwendungsschicht begrüßen den Benutzer zu einer etablierten Sitzung mit einer kurzen Statusmeldung. In dieser wird meistens auch der Name und die Versionsnummer des Daemons sowie die Plattform, der Name und die Version des Betriebssystems mitgeschickt. Diese Information ist sehr wichtig, denn anhand dieser Daten können weitere Zugriffe koordiniert und spezifische Schwachstellen gesucht und überprüft werden.

Diese Auswertungs-Zugriffe werden sowohl in der deutschen als auch in der englischen Literatur als Banner-Grabbing bezeichnet. Das Abgreifen des Banners ist wiederum sehr einfach mit einer Terminal-Emulation durchzuführen. Bei den meisten interaktiven Diensten reicht das etablieren einer Sitzung. Dies kann zum Beispiel durch die Eingabe von "telnet www.scip.ch 21" für den TCP-Port 21 (normalerweise FTP) auf dem Host mit dem Namen www.scip.ch durchgeführt werden. Sobald die Verbindung hergestellt werden konnte, begrüßt uns der FTP-Server mit seinem Willkommens-Banner. Um die FTP-Sitzung erfolgreich weiterzuführen, wäre die Authentifizierung mittels Benutzername (USER) und Passwort (PASS) notwendig. Wir sehen jedoch davon ab und beenden die Verbindung mit der Eingabe des Befehls "QUIT". Die Verbindung wird dann auf mit der höflichen FIN-Methode beendet.

```
mruef@debian~$ telnet www.scip.ch 21
Trying 192.168.0.2...
Connected to www.scip.ch.
Escape character is '^]'.
220 ProFTPD 1.1.3rc2 Server (Debian)
[www.scip.ch]
QUIT
221 Goodbye.
Connection closed by foreign host.
```

Einige Server-Anwendungen wollen jedoch prozotiert werden. Manche geben erst nach einer kurzen Aufforderung die gewünschten Informationen heraus. Bestes Beispiel hierfür HTTP. Nach etablierter Verbindung bleibt der HTTP-Daemon normalerweise stumm und wartet auf die HTTP-Anfrage des Clients. Sehr beliebt ist in diesem Zusammenhang das Absetzen einer HEAD-Anfrage im Rahmen der HTTP-Sitzung.

Dabei wird nach etablierter Sitzung mit dem HTTP-Port die Anfrage "HEAD / HTTP/1.0" übergeben. Der Server sollte sodann die Kopfdaten ohne den Inhalt zurückliefern. Vorteil dieses Zugriffs ist, dass nicht unnötig irgendwelche HTTP-Nutzdaten übertragen werden müssen. Der Zugriff erfolgt also schnell, effizient und unkompliziert. Nachteil ist jedoch, dass viele Server oder Administratoren diesen Zugriff, der wirklich nur für Auswertungen genutzt wird, nicht zu. So erhält man eine knappe Fehlermeldung, dass dieses Kommando nicht unterstützt sei. Sodann muss man auf die klassische GET-Anfrage mit all ihren Nachteilen zurückgreifen.

Erkennen des Betriebssystems

Der nächste Schritt ist das Erkennen des Betriebssystems. Dies ist in erster Linie nur dann erforderlich, wenn diese Information dem Auditoren bis dato nicht zugekommen lassen wurde. Der Nutzen dieses Tests ist, dass das weitere Vorgehen optimiert werden kann. So werden Linux-Hosts beispielsweise auf ganz andere Schwachstellen überprüft, weder die Windows-Betriebssystemreihe.

Um das auf einem Host eingesetzte Betriebssystem zu erkennen, können verschiedene Techniken eingesetzt werden. Da wir schon mit der Hilfe eines Portscans die Stati der verschiedenen Ports identifiziert haben, können wir eventuell Rückschlüsse auf das eingesetzte Betriebssystem ziehen. Die offenen Ports 135, 137, 138 und 139 sind typisch für ein Windows-Betriebssystem. Entdecken wir zusätzlich den offenen Port 445, verbirgt sich dahinter sehr wahrscheinlich ein Windows 2000 oder XP. Finden wir die Ports 23, 25, ... offen, verbirgt sich dahinter mit grösster Wahrscheinlichkeit eine Symantec Raptor-Firewall.

Eine etwas zuverlässigere, jedoch zugleich aufwendigere Methode ist im sogenannten OS-Fingerprinting gegeben. Bei dieser Methode werden die Eigenschaften der jeweiligen TCP/IP-Implementierungen zur Determinierung des eingesetzten Betriebssystems herangezogen. Aus diesem Grund wird diese Methode auch TCP/IP- oder Stack-Fingerprinting genannt. Man unterscheidet zwischen aktivem und passivem OS-Fingerprinting. Bei der aktiven Variante werden durch bestimmte Reize die gewünschten Reaktionen provoziert. Sie benötigt ein Mehr an Aufwand und Ressourcen. Ihr Vorteil ist jedoch, dass nicht auf durch andere Systeme generierten Verkehr mit dem Zielhost gewartet werden muss. Aus diesem Grund wollen wir uns an dieser Stelle nur mit den Tools für aktives Stack-Fingerprinting beschäftigen.

Die Herkunft des OS-Fingerprintings ist nicht ganz klar. Eines der ersten Tools, dass die verschiedenen Charakteristika einer TCP/IP-Kommunikation zur Identifizierung war das für Linux entwickelte Queso. Nmap liess sich jedoch nicht lange bitten und wartete bald auch mit einer solchen Funktion auf. Diese kann durch das Miteinbeziehen des Parameters -O (das O steht für OS-Fingerprinting) aktiviert werden; wahlweise mit einem Portscan oder als eigenständigen Auswertungs-Zugriff.

```
debian:~# nmap -sT -p 80,81 -O www.scip.ch
```

```
Starting nmap 3.27 ( www.insecure.org/nmap/ )
at 2003-07-03 11:29 CEST
Interesting ports on www.scip.ch
(192.168.0.2):
(The 1 port scanned but not shown below is in
state: closed)
Port      State      Service
80/tcp    open      http
Remote operating system guess: Linux Kernel
2.4.0 - 2.5.20
Uptime 247.936 days (since Mon Oct 28
12:01:54 2002)
```

```
Nmap run completed -- 1 IP address (1 host
up) scanned in 5.933 seconds
```

Nmap führt beim OS-Fingerprinting mehrere verschiedene Zugriffe durch, deren Reaktion der Gegenstelle das eingesetzte Betriebssystem verraten soll. Dabei wird eine sehr geringe Zahl an Pakete generiert - Nur wenige Intrusion Detection-Systeme sind in der Lage diesen Zugriff als solches zu identifizieren.

Sicherheitslücken identifizieren

Man muss zwischen dem Finden und dem Identifizieren von Sicherheitslücken unterscheiden. Die verschiedenen Techniken für das Finden neuer Schwachstellen und die entsprechende Vorgehensweise hier zusammenzufassen, würde den Umfang bei weitem sprengen. Wir beschränken uns daher auf das Suchen altbekannter Schwachstellen. Dies ist wirtschaftlicher, da es weniger Zeit und Aufwand in erfordert.

Könnte die auf einem Host eingesetzte Software (Anwendungen und Betriebssystem) identifiziert werden, können in verschiedenen Verwundbarkeits-Datenbanken die Schwachstellen dazu gesucht werden. Die bekannteste und umfassendste davon wird auf SecurityFocus.com bereitgestellt. Eine deutschsprachige Datenbank mit Sicherheitslücken wird von der Firma scip AG unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> publiziert. Durch verschiedene Such-Methoden lässt sich anhand des Herstellers, des Produktnamens und der Versionsnummer die Anzahl der Schwachstellen

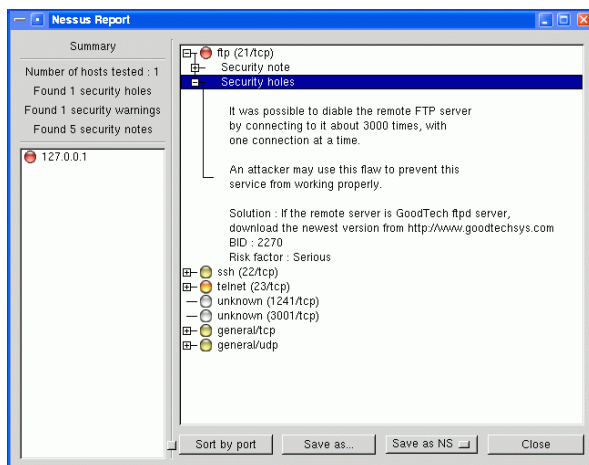
ermitteln. Jenachdem werden Informationen geliefert, wie Sicherheitslücke ausgenutzt werden kann und welche Gegenmassnahmen es gibt.

Automatisiertes Scanning

Besonders im grossen Umfeld macht es wenig Sinn, das Scanning manuell mit den zuvor beschriebenen Zugriffen durchzuführen. Gilt es ein ganzes Netzwerk systematisch nach Schwachstellen abzusuchen, kommen sogenannte Security Scanner zum zug. Diese Software vereinigt die bekannten Methoden zur Auswertung von Systemen, um anhand der gesammelten Informationen die potentiellen oder existenten Schwachstellen auszuweisen.

Es gibt eine Vielzahl verschiedener Vulnerability Scanner. Zum Beispiel ist mit der Freeware LANguard sehr einfach ein kleines Netzwerk abgescannet. Kommerzielle Lösungen wie ISS Internet Scanner oder Symantec NetRecon kommen da schon ein bisschen professioneller daher. Durch die vorgefertigten Reports lässt sich sehr schnell und unkompliziert das Problem Schwarz auf Weiss nachlesen.

Die mitunter populärste Security Scanner Lösung wurde für Linux entwickelt und nennt sich Nessus. Das open-source Projekt basiert auf dem Client/Server-Prinzip, bei dem auf einem Host der Nessus-Daemon installiert wird. Mit diesem verbindet sich der Nessus-Client, um ihn anzuweisen, welche Scans in welcher Form durchgeführt werden sollen. Der Vorteil dieses Ansatzes ist, dass verschiedene Clients unabhängig voneinander platziert den gleichen Server nutzen können.



Ein wichtiges Merkmal eines guten Vulnerability Scanners ist die Anzahl und Aktualität der durchzuführenden Checks. Da es sich bei Nessus um ein sehr populäres open-source Projekt handelt, werden praktisch täglich neue

scip monthly Security Summary
Marc Ruef & Simon Zumstein
scip_mss-19_10_2003-1.doc

Plugins nachgereicht, die sich sehr einfach installieren lassen. Ein anderer wichtiger Punkt bei Security Scannern ist die Qualität und der Umfang der am Schluss generierten Reports. Da in diesen die gefundenen Schwachstellen und die empfohlenen Gegenmassnahmen festgehalten werden, ist es unabdingbar, dass diese aktuell und leicht nachvollziehbar sind. Auch hier hat Nessus in den letzten Jahren gewaltige Sprünge nach Vorne gemacht.

Reporting

Ein wichtiger Schritt beim Security Auditing, der gerne unterschätzt oder gänzlich vergessen wird, ist das Reporting. In dieser Phase, nach dem Abschluss der jeweiligen Scans, werden die Resultate zusammengetragen und dokumentiert. Dieses Papier ist sodann die Grundlage für das Einleiten und Umsetzen der entsprechenden Gegenmassnahmen, um die Sicherheit der Umgebung zu wahren und zu stärken.

Wie der Audit Report aufgebaut ist und in welchem Umfang er daherkommt, ist den individuellen Wünschen anzupassen. Ein fünfstufiger Aufbau hat sich jedoch bewährt. In diesem wird an erster Stelle der Auftraggeber, der Auftragnehmer und die desweiteren involvierten Parteien aufgelistet. Dadurch kann auch später noch ausgemacht werden, wer für welche Punkte zuständig war. Im zweiten Teil wird in groben Zügen eine nicht-technische Zusammenfassung des Zustands durch das Management Summary vorgetragen. Dadurch kann man sich schnell und ohne tiefeschürfende Fachkenntnisse über die Lage informieren. Vor allem die Entscheidungsträger heissen diesen Teil willkommen. Desweiteren sollte die Vorgehensweise bei der Überprüfung dokumentiert werden. Dadurch kann bei einem zweiten Audit aus vergangenen Fehlern gelernt oder sich auf ältere Daten gestützt werden. Ein Grossteil des Reports macht das Auflisten sämtlicher konzeptioneller und technischen Schwachstellen aus. Dabei sollten Lösungsvorschläge unterbreitet werden, die auf die jeweilige Umgebung angewendet werden können. Die Ausgaben der Scans und die durch den Computer generierten Reports runden das Dokument ab. Anhand derer können Verifikationen durchgeführt oder zusätzliche Informationen gefunden werden.

Gegenmassnahmen umsetzen

Wir haben gesehen, dass das höchste Ziel eines Security Audits das Wahren und Stärken der Sicherheit eines Systems ist. So ist es unabdingbar, die durch das Assessment aufgedeckten Schwachstellen zu beheben. Diese Gegenmassnahmen können meistens

entweder auf technischer oder auf konzeptioneller bzw. organisatorischer Ebene angesetzt werden. Es bleibt den Entscheidungsträgern überlassen, wie ein Problem gelöst werden soll. Dies kann je nach Problem und Umgebung anders ausfallen.

Fazit

Das erfolgreiche Umsetzen von Security Audits ist in den meisten Fällen eine komplizierte und nervenaufreibende Sache. Um Problemen aus dem Weg zu gehen, sollten Vorabklärungen getätigt und der gesamte technische Teil vorbereitet werden. Sind alle Hindernisse aus dem Weg geschafft worden, gilt es auf technischer Ebene die Schwachstellen eines Systems herauszufinden. Die Vorgehensweise bleibt dabei dem Auditoren überlassen und richtet sich in erster Linie nach den Wünschen des Auftraggebers. Jenachdem kann das Assessment intensiver oder breitflächiger ausfallen. Schwachstellen lassen sich sehr gut durch manuelle Zugriffe (Auswertung und Attacke) aufspüren. Dies ist jedoch in den meisten Fällen nicht wirtschaftlich genug, so dass ein Security Scanner herangezogen werden sollte. Durch diesen kann eine Umgebung automatisiert nach etwaigen Schwachstellen abgesucht werden.

Konnte der technische Teil erfolgreich durchgeführt und gar einige konzeptionelle oder technische Schwachstellen entdeckt werden, gilt es diese in einem Report zu dokumentieren. Dieses Papier wird die Grundlage für das weitere Vorgehen, das Beheben der Schwachstellen oder Durchführen weiterer Tests, sein. Wichtig ist, dass das Beheben von Sicherheitslücken ein unabdingbarer Bestandteil eines Security Audits ist. Dieser alleine ist nämlich wertlos, da dadurch lediglich der Stand der Sicherheit eines Systems dokumentiert werden kann – Die Sicherheit ansich ist damit jedoch noch lange nicht gewährleistet.

Dazu gehört auch, dass ein System einem stetigen Wandel unterworfen ist. Neue Betriebssysteme oder Software können ganz neue Probleme schaffen. Es ist also wichtig den Security Audit in regelmässigen Abständen – zum Beispiel alle paar Monate – zu wiederholen, um den Stand der Dinge zu erfassen und Trends festzustellen. Sicherheit ist ein Prozess und kein Zustand.

Links

scip AG - Durchführung von Security Audits

<http://www.scip.ch>

Computec – Computer, Technik und Security

<http://www.computec.ch>

scip monthly Security Summary
Marc Ruef & Simon Zumstein
scip_mss-19_10_2003-1.doc

Kryptocrew – Portal zu Computersicherheit

<http://www.kryptocrew.de>

5. Linktipps

5.1 The language guide

<http://www.engin.umd.umich.edu/CIS/course.des/cis400/>

Thema: Programmierung
Kategorie: Nachschlagwerk

Aufmachung	Genügend
Umfang	Gut
Suchfunktion	Fehlt
Ergonomie	Gut
Gesamtbewertung	Gut

Mit Sprachführer ist auf dieser Website einer für Programmiersprachen gemeint. Unter der URL <http://www.engin.umd.umich.edu/CIS/course.des/cis400/> findet man eine Ansammlung der populärsten Programmiersprachen.

The Language Guide

Click on a language to find out more about it:



Dieser „Language Guide“ wurde ursprünglich von und für die Studierenden der University of Michigan — Dearborn aufgebaut. Zu allen aufgeführten Sprachen finden Sie eine Kurzversion der Geschichte der Sprache, deren Anwendungsgebiete, die wichtigsten Eigenschaften und Module, weiterführende Links, Buchreferenzen zur Sprache und ein kleines Beispielprogramm „hello world“.

Meinungen

Programmierung ist und bleibt eines der wichtigsten Instrumente der Information Technologie und der dazugehörigen Security Welt. Trotz oder gerade aufgrund der vorhandenen Massware. Diese hat viele Bedürfnisse zu befriedigen und kann nicht alle Wünsche abdecken. Ich denke da nur an Konsolidierung von Log-Dateien, automatische Sicherung der Konfigurationen, Darstellung von

Systempolicies uvm.

Fazit

In der Kürze liegt die Würze. Schnell ist man in der Lage sich einer Programmiersprache anzunähern. Als Ausgangspunkt für weitere Recherchen oder als Übersicht des Gebietes. Selbst für gestandene Programmierer kann diese Seite von Interesse sein. Denn nebst den eigenen gelernten und den davon verwandten Sprachen kann man die Ansätze der unterschiedlichen Programmiersprachen nachschlagen. Auf der Seite sind nebst Scriptsprachen auch Programmiersprachen aufgeführt.

Link

Falls Ihnen das „hello world“ Beispiel einer anderen Sprache fehlt, so navigieren Sie mal auf die Seite des Hello World Projektes <http://www2.latech.edu/~acm/HelloWorld.shtml>

6. Software-Tipps

6.1 Microsoft Software Update Services (SUS)

<http://www.microsoft.com/windowsserversystem/sus/default.mspx>

Thema: Patchmanagement
Kategorie: Utility, Security
Plattform: Microsoft Windows

Funktionalität	Gut
Technik	Gut
Ergonomie	Gut
Gesamtbewertung	Gut

Patches ist das halbe Leben eines PC Benutzers. Während dieser Vorgang auf Unix-Systemen relativ einfach automatisiert werden kann, ist dieser Vorgang auf Windows-Systemen ein wenig mühsamer. Microsoft hat mit seinen zahlenden Kunden jedoch ein Nachsehen und bietet ein Freeware-Tool an, welches sicherheitskritische Updates der Betriebssysteme installieren kann. Dieses Programm ist nicht mit dem kostenpflichtigen und umfangreicheren Microsoft Systems Management Server (SMS) zu verwechseln.

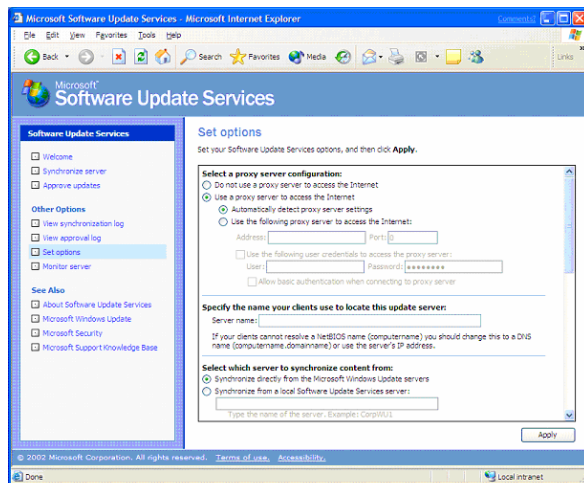
Versionen

Seit Service Pack 1 (SP1) für WinXP (sowie dem Service Pack 3 für Win2000) hat Microsoft das sogenannte Windows Automatic Update eingeführt. Dieses überprüft (je nach Konfiguration) automatisch auf der dedizierten Microsoftwebpage ob aktuelle

sicherheitskritische Patches vorhanden sind und bei Ihnen noch nicht installiert wurden. Auch der Installationsprozess kann nach einfacher Benutzerbestätigung oder automatisch (je nach Konfiguration) durchgeführt werden. Nach dem für Windows üblichen Neustart (nicht immer) ist Ihr System gepatcht.

Standard

Diese für Heimbenutzer relativ gute Möglichkeit (mit Benutzereingriff) der Patchaktivierung, ist in einem Firmennetzwerk mit mehreren Workstations eine regelrechte Denial of Service Attacke, von den vergebenen Benutzerrechten undurchführbare und aus Sicht der Zonensicherheit unzulässige Prozedur.



Herausforderung

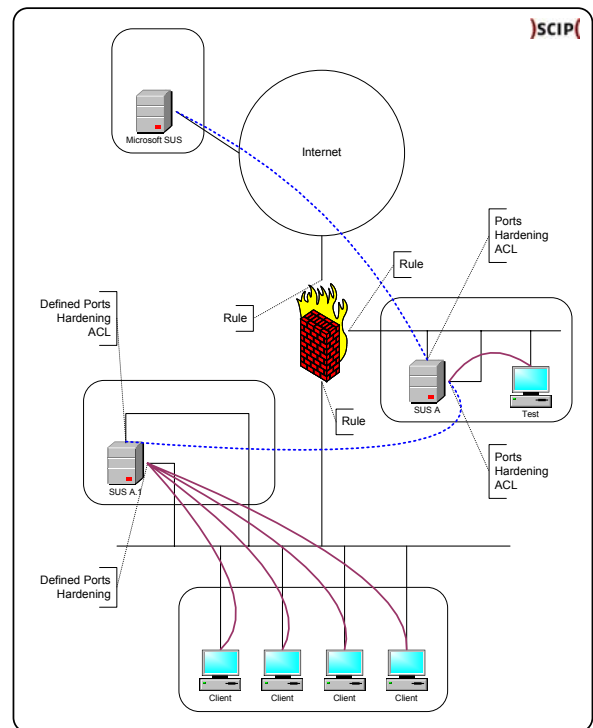
Antiviren-Hersteller standen vor einigen Jahren vor der selben Ausgangslage. Wer wollte seine Antiviren Signaturen (Patterns) schon von jedem PC einzeln herunterladen. Die Lösung war in einer Art internem Pattern-Repository gefunden. Dieses lud die aktuellsten Pattern vom Hersteller eigenen Server herunter und die internen Clients (auch Serverversionen) luden sich die aktuellste Version der Signaturen oder gar des Programmcodes vom firmeneigenen Server.

Microsoft verfolgt mit ihrem Microsoft Software Update Services (SUS) eine ähnliche Strategie. Clients oder dedizierte SUS-Workgroupserver im internen Netzwerk laden die sicherheitskritischen Updates der Betriebssysteme direkt vom internen Repository. Ohne IIS-Webserver läuft leider gar nichts. Demzufolge sind Sicherheitsmassnahmen auf dem Server vorzunehmen wie z.B. ACLs, Prozesskontrolle usw. Je nach Sicherheitskonzept innerhalb der Firma ist der SUS-Server unterschiedlich zu platzieren.

Umsetzung

scip monthly Security Summary
Marc Ruef & Simon Zumstein
scip_mss-19_10_2003-1.doc

Bei Security-Spezialisten und System Administratoren jagen autorisierte Benutzer und automatisierte Installationen Schweissperlen auf die Stirn. Hier sind grosse Angriffspunkte [Schneier 2003]. Aus sicherheitstechnischer (Sicherstellung des Ursprungs) und betrieblicher (Verhinderung von Downtime) Sicht propagieren wir die folgende Architektur.



Der Testclient (Test) stellt die Verträglichkeit und Originalität des Patches sicher. Erst nach erfolgreichem Testlauf wird der Secondary-SUS (SUS A.1) Server mit den Paketen des ersten SUS Server (SUS A) gefüttert und lässt die Clients (Client) den Update durchführen. Dieser kann dank Anwendung von mehrschichtiger Sicherheitsvorkehrung (z.B. ACL auf SUS Server und Testinstallation) automatisiert durchgeführt werden. Die Platzierung der Systeme basiert auf einem Zonenkonzept welches Datentransfer immer nur von einer Zone zur nächsten gestattet. Je nach Security Policy Ihrer Firma, sind andere Vorkehrungen zu treffen.

Zukunft

Derzeit werden weder Service Packs, noch Treiber (nicht sicherheitskritische Updates) oder Updates für Office-Produkte per SUS verteilt. Diese Funktionen könnten jedoch in der für die erste Hälfte 2004 angekündigten SUS Version 2.0 enthalten sein. Ob die Applikation dann immer noch „gratis“ sein wird, bleibt abzuwarten.

Fazit

Der Ansatz ist lobenswert. Eine

sicherheitskonforme Umsetzung birgt, wie nicht anders zu erwarten, gewisse Tücken mit sich. In diesem Fall dürfen die Sicherheitsvorkehrungen nicht vernachlässigt werden. Da bei einer Attacke auf den Standard SUS Server grosser Schaden angerichtet werden kann, insbesondere, wenn alles automatisch laufen gelassen wird (in den meisten Betrieben wohl das Ziel). Dieses darf jedoch nur unter der Anwendung der zuvor dargelegten Lösung in Betracht gezogen werden.

Der offizielle SUS_Deployguide_sp1 ist gut geschrieben und sehr umfangreich [Microsoft 2003]. Die scip AG hat eine auf Betrieb und Sicherheit abgestimmte Lösung entworfen. Diese kann modular in Ihre Umgebung eingepasst werden. Bei Interesse nehmen Sie mit uns Kontakt auf.

7. Buchtipps

7.1 Gödel, Escher, Bach – Ein unendliches geflochtenes Band

Autor: Douglas R. Hofstadter
 Verlag: DTV
 Datum: 1991
 ISBN: 3423300175
 Thema: Logik,
 Mathematik,
 Philosophie,
 Informatik
 Kategorie: Sachbuch
 Sprache: Deutsch



Lesefluss	Sehr gut
Handlungsstrang	Sehr gut
Bezug zur IT-Security	Genügend
Gesamtbewertung	Sehr gut

Was haben der Mathematiker Kurt Gödel, der Komponist Johann Sebastian Bach und der Maler Maurits C. Escher gemeinsam? Sie alle waren Genies ihrer Zeit und beglückten ihre und die nachfolgenden Generationen mit ungemein vielschichtigen, komplexen und verworrenen Gedankenanstössen.

Bis zur Unendlichkeit

Der amerikanische Informatiker Douglas R. Hofstadter versucht die Ideen seiner Helden zu kombinieren oder sie gegeneinander abzuwägen. Sein Buch mit dem Untertitel "Ein endloses geflochtenes Band" beschäftigt sich mit eben diesem Thema: Der Unendlichkeit. Am Beispiel der Kanon Bachs und den verflochtenen Bildern Eschers zeigt er die verschiedenen Darlegungen und Interpretationen dieses nicht

enden wollenden Themas.

Mathematik und ihre Grenzen

Zwischendurch macht Hofstadter einen Abstecher in das Gebiet der Logik, der Physik und Mathematik. So erläutert er, inwiefern die Mengenlehre in den 80er Jahren der Mathematik die nötige Präsenz zu verschaffen versuchte, jedoch an ihrem eigenen System scheiterte. So ist es in der Mengenlehre nicht möglich, eine Menge zu bestimmen, die alle Mengen beinhaltet. Dies hätte eine Rekursion zur Folge, die nicht vorstellbar oder gar mit der simplen Mengenlehre darstellbar wäre. Der Leser beginnt zu entdecken, dass selbst statisch erscheinende Naturwissenschaften wie die Mathematik ihre Grenzen und Widersprüche haben.



Logik kann unlogisch sein

Selbst Beispiele formaler Systeme, grammatikalischer Satzbildung oder der Lyrik versuchen den Leser in seinem Denken zu erschüttern. So gehen wir davon aus, dass die folgende Aussage wahr ist: "Ein Mensch hat fünf Finger." Ebenfalls ist die folgende Aussage wahr: "Dies hier sind fünf Wörter." Da wir die Korrektheit dieser Sätze nicht leugnen können, müsste selbst die logische UND-Verknüpfung dieser ihre Richtigkeit mit sich bringen. Doch leider ist ganz offensichtlich der zweite Teil der Aussage "Ein Mensch hat fünf Finge und dies hier sind fünf Wörter" falsch. Ein hervorragender Einstieg in das Thema der Meta-Sprachen und -Definitionen. So erfahren wir auch, weshalb man sich bei einem Flaschengeist, der einem drei Wünsche gewährt, nicht wünschen kann, dass man 100 Wünsche hat. Eine endlose Rekursion mit Paradoxitäts-Charakter wäre die Folge und würde das System in sich selbst zusammenbrechen lassen.

Das Paradoxe an der Intelligenz

Immerwieder versucht der Autor die Verbindung dieser Paradoxa mit dem Wesen der künstlichen Intelligenz herzustellen. Inwiefern ist sie denkbar, machbar und vertretbar. Ist das menschliche Gehirn tatsächlich möglich, ein Quasi-Abbild seines Selbst, mit allen Ecken und Kanten, Vorteilen und Einschränkungen zu schaffen. Mit vielen unterhaltsamen Thesen, die manchmal als Fabel-Dialog zwischen dem Herrn Schildkröte und dem Läufer Achilles ausgetragen werden, manchmal im klassischen Essay-Stil, führt der Autor den Leser Schritt für Schritt in seine komplexe Welt ein.

Fazit

Man merkt dem Buch eindeutig an, dass es gereift ist. Die Umschreibung Lebenswerk ist deshalb noch nicht mal ein Fehlgriff, denn ein Kompendium mit dieser Vielschichtigkeit, Eleganz und Selbstironie ist wahrhaftig ein Meisterwerk. So mancher Rezensent, zum Beispiel auf Amazon.de, bemängelt die Aktualität dieses Schaffens Hofstadters: Die Forschung im Bereich der Psychologie und der künstlichen Intelligenz hätte enorme Fortschritte gemacht. Dies bestreite weder ich noch der Autor. Doch "Ein endloses geflochtenes Band" ist kein Kompendium mit Anspruch auf Komplettheit und Aktualität. Viel mehr ist es eine Grundlageneinführung, die für einen Grossteil der Leserschaft den eigenen Horizont erweitert hat und erweitern haben wird. Ich kann es nur jedem empfehlen, der sich für Logik und Philosophie, künstliche Intelligenz, Mathematik und Kunst interessiert.

8. Multimedia

8.1 Fernsehen: ServiceZeit Technik – WDR Fernsehen

Anbieter: Westdeutscher Rundfunk
Köln
Redaktion: Wolfgang Back
Moderation: Angelika Schleese,
Christoph Tiegel



URL:
<http://www.wdr.de/tv/service/technik/inhalt/aktuell/>

IT-Security Beiträge	Spärlich
Inhalt	Passend

Themengebiete	Gut
Moderation	Gut
Gesamtbewertung	Gut

Multimedia hat die Welt erobert. Beinahe in jedem Gerät sitzt bereits heute ein Chip. In Zukunft werden sogar in Banknoten oder Getränkeflaschen Einwegchips zum Einsatz kommen. Die Vernetzung dieser wird ebenfalls zunehmen [scip AG 2003c].

Trotz dieser allgegenwertigen Computerisierung und der dadurch einhergehenden Abhängigkeit wird dem Thema Computer in den momentan populärsten Medien wie z.B. Television beinahe kein Sendeplatz dargeboten. Erstaunlich.

Inhalt








Die Sendung „ServiceZeit Technik“ des Westdeutschen Rundfunks (wdr) ist auf Themen aus den Bereichen Computer und Kommunikation fokussiert. Nebst Berichten über Flachbildschirme, WLANs, Navigationssysteme uvm. werden auch Themen wie die Digitale Unterschrift aufgenommen.

Fazit

Die Sendung hebt sich lobenswert von den „reisserischen“ Beiträgen in „Wissenssendungen“ Sonntagabends auf den deutschen Privatsendern ab. Die Beiträge versuchen komplexe Umstände einfach rüberzubringen. Das Neueste vom Neuesten müssen Sie nicht im Fernsehen erwarten. Dies wird immer noch über andere Kanäle verbreitet. Trotzdem sind die Beiträge dem allgemeinen Zeitgeschehen passend. Schade ist, dass unser Thema: IT-Sicherheit spärlich vertreten ist.

Bewegte Bilder geben dennoch einen Besseren Eindruck als das geschriebene Wort. Zur Vertiefung einer Aussage bleibt es jedoch dabei, Informationen finden Sie nur in Texten (Bücher, Weblogs, Mails uvm.)

9. Kreuzworträtsel

Linux: Vergleich des Inhalts von Dateien			TCP-Flagge für die häufigste Einstellung	Asia Pacific Network Information Centre		Liste für Zugangsprotokolle	Tool zum Mithlesen von Netzwerkverkehr		Les- und schreibbarer Speicher		optische Platte		Speicherresidentes Programm
DDoS-Tool			Dateisystem von Windows 9x				Nachrichtendienst der Vereinigten Staaten				verteiltes Dateisystem		
			Methodik zur Steuerung des IT-Betriebs				Protokoll für Fehler und Informationen					Wagendiebstahl	
			UNIX-Kommando äquivalent zu dir unter DOS				DOS: Vergleich des Inhalts von Dateien				Konkurrenzlösung zu PHP		Abk. Initiale Sequenznummer
Zeilenverschiebung	Lautes Lachen.			Verbindung zwischen zwei Netzen		Vorgänger von Windows 2000			Linux: Kopiert Dateien		<small>Schrittweite (Pulsweite) von u.a. 0.5µs max. 32 MHz (u.a.)</small>		
scp: Dienstleistung für Internet, kann zu Schwachstellen führen	Programmiersprache für Windows Tabellen		Remote Control Programm mit ICMP		Worum handelt es sich bei RJ-45								Einheitliche Sprache zur Kommunikation
						Künstliche Intelligenz	Prozedur aufruf auf entfernten Rechner				Abk. John the Ripper		Basiswort im Film "Password Swordfish"
			Verbündetes Transportprotokoll		Computermesse in Basel				Auf Chipkarten genutzte Verschlüsselung	<small>Domainen (auf dem Internet)</small>	Berkeley Internet Name Domain		
Internet Protocol						<small>Datenübertragung für WAN</small>					Entwickler der Z1, Z2, Z3		
Übertragungsprotokoll für Mobiltelefone	Zeichen-Codierung					Unix: Verschieben einer Datei			Konkurrenz-Prozessor zu denen von Intel				
			Häufig gestellte Fragen.										
			Unterbrechungsfreie Stromversorgung				Abk. Backup Domain Controller			Zentraleinheit eines Computers			
Abk. Javascript													
Webserver von Microsoft					Klassischer UNIX-Texteditor								

Wettbewerb

Gewinnen Sie einen Monat unserer Dienstleistung **),pallas(**, im Wert von bis zu **285CHF** (197EUR)! Die **drei** ersten Einsendungen des richtigen Lösungswortes gewinnen. Mailen Sie das erarbeitete Schlüsselwort an die Adresse <mailto:info@scip.ch>. Einsendeschluss ist der **15.11.2003**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Jede Einsendung wird persönlich kommentiert! Dieser Wettbewerbsgewinn (Packetgröße EXA und Wertauszahlung ausgeschlossen) kann auf einem bestehenden Abonnement oder einer Neuanmeldung verbucht werden.

Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

10. Literaturverzeichnis

Microsoft, Januar 2003, Deploying Microsoft Software Update Services,
http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc

Ruef, Marc, 2003, Ein Fall für Nick Knatterton – Intrusion-Detection mit Linux, Linux Enterprise, Ausgabe 11/03, <http://www.linuxenterprise.de> und <http://www.computec.ch>

Schneier, Bruce, 15. November 2003, Cryptogram, Ausgabe November 2003,
<http://www.schneier.com/crypto-gram-0309.html>, deutsche Übersetzung durch die scip AG, 19. November 2003,
<http://www.scip.ch/publikationen/crypto-gram/2003-09-15-cryptogram-de.html>

scip AG, 19. April 2003a, scip monthly Security Summary, Ausgabe 19. April, Archiv > Errata, <http://www.scip.ch>

scip AG, 19. August 2003b, scip monthly Security Summary, Ausgabe 19. August, Archiv > Errata, <http://www.scip.ch>

scip AG, 19. September 2003c, scip monthly Security Summary, Ausgabe 19. September, Archiv > Errata, <http://www.scip.ch>

11. Impressum

Herausgeber:
scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 1 445 1818
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:
Marc Ruef
Security Consultant
T +41 1 445 1812
<mailto:maru@scip.ch>
PGP:
http://www.scip.ch/firma/facts/maru_scip_ch.asc

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserung möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Anfragen bezüglich der Erstellung eines **Erfahrungsaustausch Artikels**, senden Sie bitte an die E-Mail <mailto:sizu@scip.ch>.

Die scip AG – zu 100% unabhängig - unterstützt Sie in allen Belangen einer ganzheitlichen IT-Security. Sei es bei der Aufdeckung von neuen Sicherheitslücken, der Analyse und Examinierung Ihrer IT-Landschaft, der Ausbildung Ihrer Mitarbeiter, der gezielten Informationsbeschaffung zu den Sie betreffenden Verletzbarkeiten, der Wirtschaftlichkeitsprüfung Ihrer IT-Umgebung, der Konzeption Ihrer Security Architektur oder dem Einsatz von professionellem und pragmatischem Projektmanagement.

Die ausgewiesenen Spezialisten der scip AG verfügen, in diesem sehr komplexen sowie breitgefächerten Spezialgebiet, über jahrelang erarbeitetes und angewandtes Wissen.

Nutzen Sie unsere Dienstleistungen!

Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online unter <http://www.scip.ch/publikationen/smss/>.

Der Bezug des scip monthly Security Summary ist **kostenlos**. Sie können sich mit einer Email an die Adresse smss-subscribe@scip.ch eintragen. Um sich auszutragen, senden Sie Ihr Email an die Adresse smss-unsubscribe@scip.ch