

Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Hintergrundbericht
5. Kreuzworträtsel
6. Literaturverzeichnis
7. Impressum

1. Editorial

2004 hat sich etwas geändert?

Wir schreiben das Jahr 2005, zumindest in weiten Teilen unseres Planeten Erde. Seit 2002 besteht die scip AG und seit 2003 veröffentlichen wir regelmässig den scip monthly Security Summary. Den vollendeten Jahreswechsels zum Anlass nehmend, erlaube ich mir einen kleinen und begrenzten Blick in die Vergangenheit.

Hat 2004 in der IT-Security Welt etwas verändert?

Jeden Tag befasse ich mich im Auftrag von Kunden oder aus persönlichem Interesse mit IT-Sicherheit. Sei dies nun beim Lesen eines Fachartikels oder eines Security Concepts, beim Kundenworkshop oder Projekt Kick-Off, in den internen Diskussionen oder den regelmässigen siap (security is a process) Treffen, beim verfassen eines Auditreports oder der Präsentation der Penetrations Test Ergebnisse etc.

Rückblickend auf das Jahr 2004 sticht mir vorallem eine Veränderung ins Auge.

Die Medienberichterstattungen und das

Medieninteresse rund um das Thema IT-Security war wohl nie so zahlreich wie im Jahr 2004. In allen möglichen Medien kamen Berichte, Sondersendungen, Informationsmeldungen und Hilfestellungen. Eine ansich positive Entwicklung, welche wir in der März 2004 Ausgabe des smSS prognostiziert hatten [scip2004].

Das einbinden und ins rechte Licht rücken aller Facetten des Gebiets IT-Security ist ein sehr schwieriges Unterfagen und bedarf einer Mehrzahl an Sendungen, welche aufeinander abgestimmt sein müssen.

Dieses Ziel konnte, nach meiner Meinung und in anbeacht der von mir wahrgenommenen Berichte, nicht verwirklicht werde. Ausnahmen bestätigen die Regel, zum Beispiel „@neues“ auf 3Sat, Passagen aus „Alles unter Kontrolle“ auf SFdrs oder diverse Nachrichtenblöcke zum Thema der Anfälligkeit von E-Banking Lösungen deutscher Banken.

Die Grosszahl an Berichterstattungen folgte jedoch dem gleichen Muster: Die Probleme sind

bekannt, es sind dies Q, W und T. Zur Lösung dieser installieren Sie doch die Produkte Y, F und R. Damit sind Sie sicher. Dabei ging vergessen, dass Sicherheit ein Prozess ist. Der Einsatz eines Produktes ist nicht die Lösung. 100% Gewissheit ist grundsätzlich ein Ding der Unmöglichkeit. Man kann sich nur fragen ob man das Notwendige und für seine Verhältnisse gerechtfertigte an Ressourcen aufgewendet hat um sich vor Attacken zu wappnen.



Es kann als positiv erachtet werden, dass das Thema IT-Security vermehrt in der Medienlandschaft präsent ist. Diese Anwesenheit erhöht voraussichtlich die Aufmerksamkeit der Benutzer und schützt damit uns alle. Die Reduktion des Themenbietes IT-Security auf ein paar wenige, fassbare, Aspekte und die damit einhergehende Wähnung in trügerischer Sicherheit, sehe ich als grossen Negativpunkt.

Die ersten Schritte sind gemacht, nun gilt es das Erreichte zu optimieren. Falls die Berichterstattungen im gleichen Sinn weitergeführt werden, so sehe ich die Gefahr einer Zweiklassengesellschaft in der IT-Security.

Simon Zumstein <sizu at scip.ch>
Geschäftsleiter
Zürich, 19. Januar 2005

2. scip AG Informationen

2.1 ATK-Attack Tool Kit in Japan

Das von Herrn Marc Ruef, seineszeichens Security Consultant der scip AG, programmierte und ins Leben gerufene Exploiting Framework und Security Scanner, ATK-Attack Tool Kit, erobert die Welt.

Nach grosser und überaus positiver Resonanz aus Europa und Amerika entdeckt nun auch der asiatische Raum die Vorzüge und Qualitäten des ATK. Nebst Anfragen aus Korea folgt nun gar die Publizierung im Fachguide: Hacker Japan und der beiiegenden CD „Security Tools Collection 2005“.



Detaillierte Informationen zum Projekt ATK-Attack Tool Kit finden Sie auf der Projektpage unter <http://www.computec.ch/projekte/atk>.

2.2 smSS Resdesign

Das in der Oktober 2004 Ausgabe des scip monthly Security Summary angekündigte Redesign wurde verschoben.

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 Sun Solaris 9 Kerberos V5 bis krb5-1.3.5 libkadm5srv Pufferüberlauf
- 3.2 RIM BlackBerry Enterprise Server Mobile Data Service bis 4.0 WML Denial of Service
- 3.3 ISS Proventia A, M und G RFC2397 Entdeckung umgehen
- 3.4 Check Point Firewall-1 NG SmartDefense bis 541041226 RFC2397 Entdeckung umgehen
- 3.5 Netscape Directory Server bis 6.21 LDAP-Anfragen Pufferüberlauf
- 3.6 CUPS bis 1.1.23 HTTP GET /.a Denial of Service
- 3.7 Microsoft Internet Explorer bis 6 .hhk erweiterte Rechte
- 3.8 Exim bis 4.43 SPA Authentisierung spa_base64_to_bits() Pufferüberlauf
- 3.9 Microsoft Windows bis XP mit Service Pack 2 winhlp32.exe korrupte HLP-Datei Pufferüberlauf
- 3.10 Microsoft Windows bis XP mit Service Pack 2 korrupte ANI-Datei Pufferüberlauf
- 3.11 Microsoft Windows bis XP mit Service Pack 2 LoadImage API Pufferüberlauf
- 3.12 Nokia IPSO 3.x OpenSSH Benutzer identifizieren
- 3.13 MIT Kerberos V5 bis krb5-1.3.5 libkadm5srv Pufferüberlauf
- 3.14 Netegrity SiteMinder Login TARGET-Weiterleitung Designfehler
- 3.15 Novell GroupWise WebAccess error about erweiterte Rechte
- 3.16 Novell GroupWise WebAccess error Authentisierung umgehen

3.1 Sun Solaris 9 Kerberos V5 bis krb5-1.3.5 libkadm5srv Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja
 Datum: 17.01.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1128>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen. Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Wie das MIT meldete, existiert eine Pufferüberlauf-Schwachstelle in MIT Kerberos V5 bis krb5-1.3.5. Davon effektiv betroffen ist libkadm5srv, worüber ein externer Anwender beliebigen Programmcode ausführen und so ein Kerberos-System komplett kompromittieren kann. Sun hat im Januar 2005 eben diese Verwundbarkeit in ihrem Sun Solaris 9 best'tigt. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Das MIT Kerberos Team hat einen Patch herausgebracht. Als Workaround wird empfohlen, die Passwort-History auf ein Maximum zu erweitern, um die Chancen eines erfolgreichen Angriffs zu minimieren. Das Problem wird zudem in der Version krb5-1.4 von Haus aus behoben sein. Sun selber arbeitet noch an einer Lösung.

Expertenmeinung:

Die hohe Verbreitung von Kerberos sowie die Möglichkeiten eines Angriffs machen diese Schwachstelle für eine Vielzahl an Angreifern sehr interessant. Jedoch ist das Risiko eingedämmt, da die Sicherheitslücke scheinbar nur unter gewissen Umständen ausnutzbar ist. Administratoren werden angehalten so schnell wie möglich ihre Systeme zu überprüfen und im Notfall unverzüglich Gegenmassnahmen einzuleiten. Es ist damit zu rechnen, dass in den kommenden Tagen ein Exploit erscheinen wird.

3.2 RIM BlackBerry Enterprise Server Mobile Data Service bis 4.0 WML Denial of Service

Einstufung: **problematisch**
 Remote: Ja
 Datum: 17.01.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1125>

BlackBerry ist eine kommerzielle Mobile-Lösung aus dem Hause Research In Motion Limited (RIM). Durch entsprechende BlackBerry-Handhelds kann stets ein Abgleich mit dem Enterprise Server umgesetzt werden, um stets bezüglich Emails und Terminen auf dem neuesten Stand zu sein. Zusätzlich werden auch

Dienste für SMS, Webbrowser und Telefonie angeboten. Der Hersteller meldet eine Denial of Service-Schwachstelle im Verarbeiten von WML-Kommunikationen (Wireless Markup Language), bei denen eine URL ohne Leerzeichen im Kommentar-Block gegeben ist. Dies führt im System zu einer Auslastung von 100 %. RIM hat Patches für einige der betroffenen Server-Versionen herausgegeben. Patches für 4.0 sind noch nicht vorhanden.

Expertenmeinung:

Das BlackBerry-System ist auf dem Vormarsch und erste grossflächige Evaluierungen bzw. Integrationen haben begonnen. Schwachstellen wie diese fördern natürlich nicht den Verkauf der RIM-Lösung. Jedoch ist ein schnelles Ausmerzen von Schwachstellen ein gutes Zeichen und deutet auf Kompetenz des Herstellers hin. So bleibt zu hoffen, dass die Patches für die Versionen 4.0 ebenfalls noch diese Tage publiziert werden.

3.3 ISS Proventia A, M und G RFC2397 Entdeckung umgehen

Einstufung: **kritisch**
Remote: Ja
Datum: 10.01.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1120>

ISS Proventia ist ein Intrusion Prevention-System (IPS), das frühzeitig Angriffe erkennen und durch eine Limitierung der Funktion des Betriebssystems diese rechtzeitig verhindern können soll. Wie nun gemeldet wurde, existieren in zahlreichen Sicherheitslösungen ein Designfehler. Dieser erlaubt es, dass Daten nach RFC2397 nicht richtig überprüft und gefiltert werden. Durch das Einbetten encodierter Daten in HTML-Dokumenten können entsprechende Evasion-Attacken umgesetzt werden. Ein proof-of-concept Exploit des JPEG-Pufferüberlaufs von Microsoft Windows wurde zusammen mit dem Initial-Advisory veröffentlicht [<http://www.kotik.com/exploits/09222004.ms04-28-cmd.c.php>]. Als Workaround wird empfohlen, die Sicherheit nicht nur von solchen Lösungen abhängig zu machen. Das Patchen von Systemen sowie das Nutzen zusätzliche Firewalling- und Antiviren-Lösungen bleibt weiterhin unumgänglich.

Expertenmeinung:

Wie Secunia ganz richtig in ihren Meldungen vermerkt, handelt es sich hier eigentlich nicht um eine total neue Erkenntnis. Es sind eine Vielzahl an Möglichkeiten bekannt, wie derlei Systeme ausgetrickst werden können. Die Schwachstelle ist aber dennoch sehr brisant, da der

Mechanismus nach RFC2397 sehr populär ist und von einer Vielzahl an Anwendungen unterstützt wird (z.B. die populären Webbrowser und Mailclients). Firefox, Safari, Mozilla und Opera sind betroffen, wobei der Microsoft Internet Explorer nicht mit RFC2397 umgehen kann.

3.4 Check Point Firewall-1 NG SmartDefense bis 541041226 RFC2397 Entdeckung umgehen

Einstufung: **kritisch**
Remote: Ja
Datum: 10.01.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1119>

Checkpoint Firewall-1 ist eine populäre Firewall-Lösung aus dem Hause Checkpoint Software Technologies. Wie nun gemeldet wurde, existieren in zahlreichen Sicherheitslösungen ein Designfehler. Dieser erlaubt es, dass Daten nach RFC2397 nicht richtig überprüft und gefiltert werden. Durch das Einbetten encodierter Daten in HTML-Dokumenten können entsprechende Evasion-Attacken umgesetzt werden. Ein proof-of-concept Exploit des JPEG-Pufferüberlaufs von Microsoft Windows wurde zusammen mit dem Initial-Advisory veröffentlicht [<http://www.kotik.com/exploits/09222004.ms04-28-cmd.c.php>]. Als Workaround wird empfohlen, die Sicherheit nicht nur von solchen Lösungen abhängig zu machen. Das Patchen von Systemen sowie das Nutzen zusätzliche Firewalling- und Antiviren-Lösungen bleibt weiterhin unumgänglich.

Expertenmeinung:

Wie Secunia ganz richtig in ihren Meldungen vermerkt, handelt es sich hier eigentlich nicht um eine total neue Erkenntnis. Es sind eine Vielzahl an Möglichkeiten bekannt, wie derlei Systeme ausgetrickst werden können. Die Schwachstelle ist aber dennoch sehr brisant, da der Mechanismus nach RFC2397 sehr populär ist und von einer Vielzahl an Anwendungen unterstützt wird (z.B. die populären Webbrowser und Mailclients). Firefox, Safari, Mozilla und Opera sind betroffen, wobei der Microsoft Internet Explorer nicht mit RFC2397 umgehen kann.

3.5 Netscape Directory Server bis 6.21 LDAP-Anfragen Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 11.01.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1112>

Der Netscape Directory Server ist ein auf LDAP ausgelegter, zentraler Verzeichnis-Dienst. Auf diesem werden Benutzereinstellungen, Profile, Gruppen-Informationen und Zugriffskontrolllisten gespeichert

[http://enterprise.netscape.com/products/identsvc/s/directory_ds.html]. Das Red Hat Team entdeckte einen Fehler bei der Verarbeitung von LDAP-Anfragen. So sei es möglich, eine Denial of Service-Angriffe oder gar beliebigen Programmcode über einen Pufferüberlauf auszuführen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Laut US-CERT könnte sich der Fehler aber auch in den LDAP-Implementierungen anderer Hersteller finden. Produkte von Juniper Networks, Lotus Software und OpenLDAP sind jedoch nicht verwundbar. Das Red Hat Security Response Team stellt Patches in Form von aktualisierten Libraries zur Verfügung. Ein offizieller Patch von Seiten Netscape ist nicht bekannt.

Expertenmeinung:

Sonderbar an dieser Schwachstelle ist, dass das Red Hat Security Response Team Patches zur Verfügung stellt, Netscape damit jedoch noch nicht nachgezogen hat. Es bleibt zu hoffen, dass zur Wahrung der Professionalität dieser Schritt schnellstmöglich umgesetzt wird. Die Kunden werden es Netscape danken.

3.6 CUPS bis 1.1.23 HTTP GET /..a Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 30.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1100>

Linux ist ein freies, UNIX-ähnliches Betriebssystem, das der General Public License (GPL) unterliegt. Es wurde 1991 vom Finnen Linus Torvalds ins Leben gerufen. Heute gilt es als grösster Konkurrent zum kommerziellen Windows-Betriebssystem aus dem Hause Microsoft. CUPS ist der Name eines Print-Spoolers, der standardmässig bei vielen Linux-Distributionen - zum Beispiel Red Hat - mitinstalliert wird. Er arbeitet single-threaded - Ist somit lediglich in der Lage, eine Aufgabe auf einmal zu bewältigen. Es wurde nun eine Denial of Service-Schwachstelle in CUPS bis 1.1.23 entdeckt. Durch die simple HTTP-Anfrage "GET /..a HTTP/1.1" kann die CPU-Auslastung in die Höhe getrieben werden. Das Problem wurde in CUPS 1.1.23 behoben.

Expertenmeinung:

Diese Schwachstelle ist in erster Linie ärgerlich, denn durch den Denial of Service-Zugriff lässt sich der Betrieb ziemlich einfach stören. Administratoren sollten deshalb auf der Hut sein. Nicht funktionierende Unix/Linux Druckerserver deuten auf einen Angriff hin. So oder so sollte man bei seinen verwundbaren Systemen die Patches einspielen, um sich nicht doch noch herumärgern zu müssen.

3.7 Microsoft Internet Explorer bis 6 .hkk erweiterte Rechte

Einstufung: **kritisch**
Remote: Ja
Datum: 07.01.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1098>

Der Microsoft Internet Explorer ist mit seiner Verbreitung von schätzungsweise 95 % der mitunter populärste Webbrowser der aktuellen Stunde. Seine hohe Verbreitung ist unter anderem darauf zurückzuführen, dass er ein fester Bestandteil moderner Windows-Betriebssysteme ist. http-equiv entdeckte die Möglichkeit, über einen hkk-Link erweiterte Rechte auf einem Microsoft Internet Explorer bis 6 zu erlangen. Lokale HTML-Dokumente lassen sich ausführen oder Script-Injection in zuvor geladenen Dokumenten provozieren. Als Workaround sollte Active Scripting abgeschaltet werden. Alternativ kann ein anderer Webbrowser - zum Beispiel Mozilla Firefox - eingesetzt werden.

Expertenmeinung:

Es beweist sich scheinbar einmal mehr, als sei Microsoft ein grundsätzlicher Designfehler beim Entwickeln des Sicherheitsmodells für JavaScript unterlaufen. Aus Sicherheitsgründen sollten Sie Active Scripting für sämtliche Inhalte verbieten und dann vorzu benötigte Webseiten freizuschalten. Diese Herangehensweise hat sich schon seit vielen Jahren beim Erstellen von Firewall-Regeln bewährt. Nur so können Sie mit dem Internet Explorer auf der sicheren Seite sein.

3.8 Exim bis 4.43 SPA Authentisierung spa_base64_to_bits() Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 06.01.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1094>

Exim ist ein Mail Transfer Agent (MTA), der an der University of Cambridge entwickelt wird und mit sehr vielen Linux-Distributionen (vor allem Debian) ausgeliefert wird. Das Exim Team meldete zwei Sicherheitslücken in Exim bis 4.43. Eine davon ist in der Funktion `spa_base64_to_bits()` gegeben. Ein Angreifer kann bei einer SPA Authentisierung beliebigen Programmcode ausführen lassen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Das Exim Team hat das Problem mit einem Patch im CVS Repository behoben.

Expertenmeinung:

Das erfolgreiche Ausnutzen dieses Angriffs setzt die Unterstützung von SPA Authentisierungen am Zielsystem voraus. Dies könnte zu einem echten Problem für Exim-Systeme, vorwiegend Debian-Umgebungen, werden. Das Umsetzen von Gegenmassnahmen ist deshalb dringendst anzuraten.

3.9 Microsoft Windows bis XP mit Service Pack 2 winhlp32.exe korrupte HLP-Datei Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 20.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1088>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Es existieren Versionen für den Einsatz als Server und solche für den Workstation-Betrieb. Flashsky meldete gleich mehrere kritische Sicherheitslücken in Microsoft Windows bis XP mit Service Pack 2. Eine davon ist durch eine Pufferüberlauf-Angriffe mittels einer korrupten HLP-Datei gegeben. Ein Angreifer kann so über die Applikation `winhlp32.exe` beliebigen Programmcode ausführen lassen. Zusammen mit dem Advisory wurden auch zwei Exploits - einen Heap und einen Integer Overflow - publiziert. Microsoft hat noch keine Lösung für das Problem, wird aber voraussichtlich in den kommenden Monaten mit einem Patch reagieren. In der Zwischenzeit wird empfohlen, keine HLP-Dateien unbekannter oder zweifelhafter Herkunft zu öffnen.

Expertenmeinung:

Diese Schwachstelle ist in erster Linie ärgerlich, denn durch den Denial of Service-Zugriff lässt sich der Betrieb ziemlich einfach stören. Benutzer sollten deshalb auf der Hut sein, denn

Spam-Mails oder Viren könnten den Umstand nutzen, um ihren Schabernack zu betreiben. Gegenmassnahmen, das Einspielen des Service Pack 2 für Microsoft Windows XP, sind deshalb im Zusammenhang mit den anderen Schwachstellen ein Muss.

3.10 Microsoft Windows bis XP mit Service Pack 2 korrupte ANI-Datei Pufferüberlauf

Einstufung: **sehr kritisch**
Remote: Ja
Datum: 20.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1087>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Es existieren Versionen für den Einsatz als Server und solche für den Workstation-Betrieb. Flashsky meldete gleich mehrere kritische Sicherheitslücken in Microsoft Windows bis XP mit Service Pack 2. Eine davon ist durch eine vermeintliche Denial of Service-Angriffe mittels einer korrupten ANI-Datei gegeben. Das System kommt entweder zum Stillstand oder wird neu gestartet. Zusammen mit dem Advisory wurde auch ein Exploit publiziert. Rund drei Wochen später wurde von Berend-Jan Wever ein Exploit publiziert, mit dem sich gar ein Pufferüberlauf erzwingen und darüber beliebiger Programmcode einschleusen lässt. Microsoft hat dem Problem mit dem Service Pack 2 für Microsoft Windows XP Rechnung getragen.

Expertenmeinung:

Diese Schwachstelle ist in erster Linie ärgerlich, denn durch den Denial of Service-Zugriff lässt sich der Betrieb ziemlich einfach stören. Als jedoch die Pufferüberlauf-Möglichkeiten bekannt wurden, nahm die Anzahl der entsprechenden Angriffe gleich noch mehr zu. Benutzer sollten deshalb in höchstem Masse auf der Hut sein, denn Spam-Mails oder Viren könnten den Umstand nutzen, um Systeme zu kompromittieren. Gegenmassnahmen, das Einspielen des Service Pack 2 für Microsoft Windows XP, sind deshalb im Zusammenhang mit den anderen Schwachstellen ein Muss.

3.11 Microsoft Windows bis XP mit Service Pack 2 LoadImage API Pufferüberlauf

Einstufung: **sehr kritisch**
Remote: Ja
Datum: 20.12.2004

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1086>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Es existieren Versionen für den Einsatz als Server und solche für den Workstation-Betrieb. Flashsky meldete gleich mehrere kritische Sicherheitslücken in Microsoft Windows bis XP mit Service Pack 2. Eine davon ist gar sehr kritisch, betrifft sie denn die LoadImage API, die gegen einen Pufferüberlauf verwundbar ist. Ein Angreifer kann über ein fehlerhaftes Bild, Icon oder Cursor entsprechenden Programmcode ausführen. Zusammen mit dem Advisory wurde auch ein Exploit publiziert. Microsoft hat dem Problem mit dem Service Pack 2 für Microsoft Windows XP Rechnung getragen.

Expertenmeinung:

Der Angriff lässt sich ebenfalls über den Webbrowser umsetzen und ist deshalb mindestens so gefährlich, wie der vor einiger Zeit für Aufsehen sorgende JPEG Exploit. Gegenmassnahmen, das Einspielen des Service Pack 2 für Microsoft Windows XP, sind deshalb ein Muss.

3.12 Nokia IPSO 3.x OpenSSH Benutzer identifizieren

Einstufung: **kritisch**
Remote: Ja
Datum: 24.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1083>

Nokia IPSO steht für IP Security Operating System. Es stellt ein speziell gesichertes, von Nokia für ihre Hardware entwickeltes und vertriebenes, Unix-ähnliches Betriebssystem dar. Der Hersteller bestätigte eine schon länger bekannte Schwachstelle in Nokia IPSO 3.x. Unter Umständen ist es einem Angreifer möglich, existente Benutzer über OpenSSH zu determinieren. Der Hersteller will angeblich keinen Patch herausgeben und empfiehlt den Benutzern lediglich, Zugriffe auf OpenSSH mittels Firewalling zu limitieren.

Expertenmeinung:

Die Reaktion von Nokia ist ein bisschen arrogant und hätte durchaus professioneller ausfallen können. Vor allem, wenn es um eine Lösung geht, die vorwiegend in grösseren Umgebungen - auch Banken - ihren Einsatz findet.

3.13 MIT Kerberos V5 bis krb5-1.3.5

libkadm5srv Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 20.12.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1078>

Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen. Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Wie das MIT meldet, existiert eine Pufferüberlauf-Schwachstelle in MIT Kerberos V5 bis krb5-1.3.5. Davon effektiv betroffen ist libkadm5srv, worüber ein externer Anwender beliebigen Programmcode ausführen und so ein Kerberos-System komplett kompromittieren kann. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Das MIT Kerberos Team hat einen Patch herausgebracht. Als Workaround wird empfohlen, die Passwort-History auf ein Maximum zu erweitern, um die Chancen eines erfolgreichen Angriffs zu minimieren. Das Problem wird zudem in der Version krb5-1.4 von Haus aus behoben sein.

Expertenmeinung:

Die hohe Verbreitung von Kerberos sowie die Möglichkeiten eines Angriffs machen diese Schwachstelle für eine Vielzahl an Angreifern sehr interessant. Jedoch ist das Risiko eingedämmt, da die Sicherheitslücke scheinbar nur unter gewissen Umständen ausnutzbar ist. Administratoren werden angehalten so schnell wie möglich ihre Systeme zu überprüfen und im Notfall unverzüglich Gegenmassnahmen einzuleiten. Es ist damit zu rechnen, dass in den kommenden Tagen ein Exploit erscheinen wird.

3.14 Netegrity SiteMinder Login TARGET-Weiterleitung Designfehler

Einstufung: **kritisch**
Remote: Ja
Datum: 17.01.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1022>

Marc Ruef des schweizer Sicherheitsunternehmens scip AG fand bei einem Penetration Test eine Schwachstelle in Netegrity SiteMinder. Verbindet sich ein Benutzer auf eine entsprechende Login-Seite, führt diese ein lokales Forwarding durch. Bei diesem wird in der URL zusätzliche Parameter angehängt. Unter anderem ist auch eine TARGET-Spezifizierung zu finden. Diese gibt eine URL als Ziel an, die nach der Authentisierung aufgerufen

werden soll. Ein Angreifer kann nun eine entsprechende URL generieren, die nach der Authentisierung auf eine andere Webseite führt (z.B. Eine mit pornografischem Inhalt). Eine Beispiel-URL wäre

https://www.scip.ch/siteminderagent/pwcgi/smpw_servicescgi.exe?

TARGET=<http%3a%2f%2fwww%2ecomputec%2ech> - Unter anderem sind so Social Hacking bzw. Phishing Attacken möglich. Netegrity wurde am 14. Dezember 2004 per Email über die Schwachstelle informiert. Nach einer unproduktiven Rücksprache mit dem Hersteller wurde das Anliegen nocheinmal klar am 23. Dezember 2004 vorgelegt. Ohne Ergebnis. Es ist nun nach Veröffentlichung der Schwachstelle damit zu rechnen, dass das Problem in den kommenden Wochen mit einem Patch behoben werden wird. Als Workaround wird empfohlen, den Web-Zugriff zusätzlich mittels Firewalling zu schützen, um Login-Versuche unbekannter Herkunft gar nicht erst möglich sind.

Expertenmeinung:

Automatische Weiterleitungen sind vor allem in einer Zeit, in der Phishing-Attacken hoch im Kurs sein, eine gefährliche Sache. Durch das Anzeigen vermeintlich legitimer Links können Benutzer auf andere Seiten gelockt und dadurch Angriffe umgesetzt werden. Automatische Weiterleitungen sollten deshalb sehr restriktiv funktionieren (z.B. Nur für eigene Domain) oder gar nicht erst manuell spezifizierbar sein.

3.15 Novell GroupWise WebAccess error about erweiterte Rechte

Einstufung: **kritisch**

Remote: Ja

Datum: 17.01.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1021>

Novell GroupWise WebAccess ist eine kommerzielle Lösung zur Anbindung von Groupware-Lösungen über das World Wide Web (WWW). Benutzer sehen sich in der Lage, bequem über ein Web-Interface auf ihre Groupware-Lösung zuzugreifen, Emails zu Schreiben und Kalender-Einträge einzusehen [<http://webaccess.novell.com/>]. Marc Ruef des schweizer Sicherheitsunternehmens scip AG fand bei einem Penetration Test eine Schwachstelle in Novell GroupWise WebAccess. Über die Eingabe der URL <https://www.scip.com:1444/servlet/webacc?error=about> kann ohne Authentisierung die About-Information der WebAccess-Lösung eingesehen werden. Diese Information kann für spezifische Angriffe genutzt werden. Bei diesem About-

Frame wird in der Zeile Userid der Benutzername des letzten Login-Versuchs angezeigt. Durch fehlerhafte Angaben könnte Social Engineering oder eine HTML Injection umgesetzt werden. Normale HTML-Tags werden im Gegensatz zu Script-Tags zur Umsetzung effektiver Cross Site Scripting-Attacken nicht gefiltert. Novell wurde am 9. Dezember 2004 per Email über die Schwachstelle informiert. Es ist damit zu rechnen, dass das Problem in den kommenden Wochen mit einem Patch behoben werden wird. Als Workaround wird empfohlen, den WebAccess-Zugriff zusätzlich mittels Firewalling zu schützen, um Login-Versuche unbekannter Herkunft gar nicht erst möglich sind.

Expertenmeinung:

Der ungesicherte Aufruf von Dateien über eine Web-Applikation ist stets gefährlich. Oft werden dabei spezielle Eingaben wie codierte Zugriffe auf andere Dateien oder die Selbstreferenzierung vergessen. Dieser Umstand hat schon in so mancher Web-Anwendung dazu geführt, dass Authentisierungen umgangen und unerlaubte Zugriffe umgesetzt werden konnten. Das manuelle Spezifizieren von zu ladenden Dateien sollte deshalb in jeder Server-Anwendung Tabu sein.

3.16 Novell GroupWise WebAccess error Authentisierung umgehen

Einstufung: **kritisch**

Remote: Ja

Datum: 17.01.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1020>

Novell GroupWise WebAccess ist eine kommerzielle Lösung zur Anbindung von Groupware-Lösungen über das World Wide Web (WWW). Benutzer sehen sich in der Lage, bequem über ein Web-Interface auf ihre Groupware-Lösung zuzugreifen, Emails zu Schreiben und Kalender-Einträge einzusehen [<http://webaccess.novell.com/>]. Marc Ruef des schweizer Sicherheitsunternehmens scip AG fand bei einem Penetration Test eine Schwachstelle in Novell GroupWise WebAccess. Wird eine Authentisierung mit falschem Benutzernamen/Passwort vorgenommen, lädt die Web-Applikation webacc eine entsprechende Fehlerseite. Diese kann jedoch auch manuell über den Parameter error beim URL-Aufruf spezifiziert werden. Durch eine Selbstreferenzierung der Applikation - zum Beispiel

<https://www.scip.com:1444/servlet/webacc?error=webacc> - kann eine authentifizierte Sitzung

vorgetäuscht werden. Der Angreifer ist sodann mit einem "Ghost User" eingeloggt, der kein Profil aufweist und weder Daten lesen noch speichern kann. Es ist ebenfalls der Aufruf anderer Sub-Templates - zum Beispiel <https://www.scip.com:1444/servlet/webacc?error=send> für den Versand von Emails - möglich. Der Aufruf kann jedoch nur für Dateien innerhalb des Web-Verzeichnisses, die zudem die Dateierweiterung `htt` aufweisen, umgesetzt werden. Über die Eingabe der URL <https://www.scip.com:1444/servlet/webacc?error=about> ist ebenfalls die Version der installierten WebAccess-Lösung einsehbar. Diese Information kann für spezifische Angriffe genutzt werden. Das Problem besteht jedoch primär darin, dass ein Angreifer eventuell eine Schwachstelle im Produkt ausnutzen kann, die nur durch authentifizierte Benutzer ausgenutzt werden könnte. Novell wurde am 9. Dezember 2004 per Email über die Schwachstelle informiert. Es ist damit zu rechnen, dass das Problem in den kommenden Wochen mit einem Patch behoben werden wird. Als Workaround wird empfohlen, den WebAccess-Zugriff zusätzlich mittels Firewalling zu schützen, um Login-Versuche unbekannter Herkunft gar nicht erst möglich sind.

Expertenmeinung:

Der ungesicherte Aufruf von Dateien über eine Web-Applikation ist stets gefährlich. Oft werden dabei spezielle Eingaben wie codierte Zugriffe auf andere Dateien oder die Selbstreferenzierung vergessen. Dieser Umstand hat schon in so mancher Web-Anwendung dazu geführt, dass Authentisierungen umgangen und unerlaubte Zugriffe umgesetzt werden konnten. Das manuelle Spezifizieren von zu ladenden Dateien sollte deshalb in jeder Server-Anwendung Tabu sein.

4. Hintergrundbericht

4.1 Vom Kern der Intelligenz (2/2)

Essay zum philosophischen Aspekt der künstlichen Intelligenz

Marc Ruef

Die Entwicklung eines künstlichen Charakters

Die logische Gewichtung ermöglichte die Entwicklung eines individuellen Charakters der Applikation. Umso mehr mit der Anwendung kommuniziert wurde, umso ausgeprägter wurden die jeweiligen Eigenschaften, die durch den Anwender vererbt wurden. In der Lernpsychologie wird dies „Lernen am Modell“ genannt (vgl. Norbert Pohlmann „Lernfall Agression“). Menschen - in diesem Fall eine Maschine - schauen sich das Vorgehen bei anderen ab, um es zu imitieren. Dies ist in erster Linie bei Tieren gegeben, die zum Beispiel von ihren Artgenossen das Jagen, Fressen oder Fliegen abschauen. Aber auch bei Kleinkindern und Jugendlichen spielen Lernfaktoren bei der Entwicklung der Persönlichkeit eine wichtige Rolle.

Soziale und emotionale Intelligenz

In einer Phase, in der ich mich sehr intensiv mit Neuropsychologie, Bewusstsein und Intelligenz auseinandergesetzt habe, vertrat ich die Meinung, dass wahre und anstrebbare Intelligenz die emotionale Intelligenz sei. Als Alternative zum Intelligenzquotienten „IQ“ hat sich in der Psychologie der Begriff des emotionalen Intelligenzquotienten „EQ“ eingebürgert. Bei dieser geht es darum, sozial zu funktionieren, der Gruppe einen Vorteil verschaffen zu wollen, ohne sich selber dabei zu sehr zu benachteiligen. (vgl. Howard Gardner, „Frames of Mind: The Theory of Multiple Intelligences“, Basic Books, ISBN 0-465-02510-2).

Ein solches soziales Verhalten ist meines Erachtens von der Erziehung und von den gegenwärtigen Entwicklungen im sozialen System abhängig. Wer eine gute Kinderstube genossen hat, jedoch in einer sehr kaltherzigen Umgebung bestehen muss, wird sich voraussichtlich ebenfalls nicht sehr zurückhalten geben.

Die Frage ob und inwiefern emotionale Intelligenz bei unserem ChatBot mitwirkt, ist bei näherer Betrachtung nichtig. Ein passives

Mitwirken ist sowieso gegeben, da die Kommunikationen analysiert und verinnerlicht werden. Wird in einer Situation durch einen Benutzer sehr hitzig reagiert, wird auch die Software in einer ähnlichen Lage etwas ausfallend daherkommen können. Die Chancen sind aber relativ hoch, dass die gleiche oder ähnliche Situationen sich oft wiederholen und in den meisten Fällen mit Anstand durch den Anwender gelöst werden. Aufgrund der logischen Gewichtung von Reaktionen wird auch die Applikation lernen, sich normal einem Problem zu stellen.

Man könnte nun jedoch die Position einnehmen, dass die Starrheit aufgrund der Vererbung von Reaktionen, die zuvor in total anderem Zusammenhang hervorgebracht wurde, eben genau den Mangel an emotionaler Intelligenz beweise. Da möchte ich dagegenhalten, dass emotionale Intelligenz ebenso gelernt werden muss. Auch ein Mensch muss zuerst lernen – vorwiegend wieder am Modell – welche Handlungen und Reaktionen von der Gesellschaft, einer Gruppe oder einem Individuum als angemessen betrachtet werden. Aufgrund der logischen Gewichtung von Reaktionen, die wir beim neuen ChatBot eingeführt haben, ist mittel- und längerfristig auch hier die Möglichkeit einer Einpendelung gegeben.

Absichtlich verärgern kann man die Anwendung nur, wenn sie sich dessen auch bewusst ist. Werden ihr Schimpfworte an den Kopf geworfen, die sie nicht versteht, da sie diese noch nie in einem vorangegangenen Gespräch mitbekommen hat, wird sie sich in ihrer Naivität auch nicht aus der Ruhe bringen lassen. Beim Menschen ist dies nicht viel anders. Werde ich in einer Sprache beschimpft, derer ich nicht mächtig bin, werde ich auf non-verbaler Ebene die Intention des Geschehnisses deuten müssen. Unter Umständen schätze ich die Situation falsch ein, weshalb eine ansonsten hervorgebrachte Verärgerung durchaus ausbleiben könnte.

Limitierung der biologischen Menschlichkeit

Bisher klingt alles sehr gut. Wir haben ein an der Natur angelehntes Reaktions- sowie Lernmodell, die unserer Applikation schon sehr menschliche Züge verleihen. Trotzdem mutet das Gerät mechanisch an und irgendwie, so scheint es, kann doch von Menschlichkeit keine Rede sein. Dies mag zum Teil stimmen. Dabei lässt man jedoch ausser Acht, dass bei einer solchen Lösung wie bei dieser mit Web-Frontend auf die Emulation anderer menschlicher Züge verzichtet

wurde.

Die Kommunikation findet ausschliesslich über Tastatur und Bildschirm statt. Der Computer macht dabei keinen Anschein, als sei er ein lebendiges Wesen. Dies ist auch nicht das primäre Ziel des Vorhabens. Es gilt lediglich darum, die menschliche Intelligenz/Reaktion zu simulieren. Man muss sich bei der Kommunikation mit dem ChatBot vorstellen, als sei nicht der Computer das Gegenüber, sondern ein "Mensch", der am anderen Ende einer Datenleitung sitzt - So wie bei einem Chat im Internet, bei dem der Computer lediglich ein Medium ist.

Dies ist auch das Hauptanliegen eines Turing-Tests, der 1950 vom berühmten Informatiker Alan Turing als Kriterium zur Erkennung der Intelligenz eines Computers vorgeschlagen wurde. diesem Test lässt man eine Testperson über eine Tastatur und einen Bildschirm ohne Sicht- oder Hörkontakt mit zwei ihm unbekanntem Gesprächspartnern ein Gespräch führen: Der eine Gesprächspartner ist ein Mensch, der andere eine Maschine. Wenn die Testperson die Gesprächspartner nicht auseinanderhalten kann, hat die Maschine den Turing-Test bestanden. (vgl. Alan Turing „Computing Machinery and Intelligence“, Mind, vol. LIX, no. 236, October 1950, pp. 433-460)

Der Preis der Kategorie "Turing-Test bestanden" wurde zwar im alljährlichen Loebner Prize (<http://www.loebner.net/Prize/loebner-prize.html>) noch nie verliehen, jedoch bin ich der festen Überzeugung, dass der ChatBot in der neuen Fassung diesen Test, nach entsprechend langer Lernphase, theoretisch zu bestehen in der Lage sein müsste. Wie lange und intensiv diese Phase sein müsste, lässt sich nur sehr schwer abschätzen. Da unbekannte Themen für die Applikation Neuland sind, werden auf diesen Gebieten vor allem zu Beginn praktisch keine Dialoge möglich sein. Fortwährend würde der ChatBot nach möglichen Antworten fragen, um dadurch seine Datenbank zu erweitern. Aber bedenken wir, dass auch ein Kind im Vorschulalter nur schwerlich den Turing-Test bestehen könnte. Dies würde den Trugschluss zulassen, dass ein Kind keine Intelligenz – wenigstens nach Turing – besitzt.

Grundgesetze der umfassenden Intelligenz

Wir haben gesehen, welche Mechanismen bei meinem Projekt zum Einsatz kamen, um zu funktionieren (Reiz/Reaktion) und um zu lernen (dynamische Datenbank mit logischer Gewichtung). Dabei stellte sich für mich

immerwieder die Frage, was denn nun die Grundlagen des Ichs sind, was sind die Grundlagen, aus denen sich Intelligenz entwickeln kann, wieviel Vorgaben muss in Form von fest verdrahteten Reaktionen gemacht werden?

Diese Vorgaben werden bei Mensch und Tier als Instinkte bezeichnet. Sind sind wichtigster Bestandteil für das Überleben und dadurch auch für die Weiterentwicklung. Jedes Kleinkind weiss schon lange, bevor es laufen oder sprechen kann, wie die Nahrungsaufnahme funktioniert. Ebenso ein Häschen, das ebenso ohne die Möglichkeit des Lernen am Modells weiss, wie die Fortpflanzung funktioniert. Und seien wir mal ehrlich: Letzteres erscheint in seiner Ausübungsweise eigentlich nicht unbedingt offensichtlich.

Die "Instinkte" meiner Applikation sind mit Sicherheit die Module für das Verarbeiten von Ein- und Ausgaben. Ebenso natürlich das Verwalten, Auswerten und Erweitern der Datenbank. Wir können also zusammenfassen, dass ein System folgende Eigenschaften mitbringen muss, um Intelligenz entwickeln zu können¹:

1. auf Reize adäquat reagieren können
2. sich wundern bzw. fragen können
3. neue Reize/Reaktionen aufnehmen können

Es stellte sich für mich nun die Frage, ob und inwiefern diese "Instinkte" der Intelligenz reduziert werden können. Ist es möglich, Intelligenz entwickeln zu können, indem lediglich einer der Punkte fest verdrahtet werden muss - Die anderen sollten sich sodann aus diesem entwickeln können. Bisher lautet die Frage auf diese Antwort Nein. Ein System, das lediglich Punkt 1 mit Reiz/Reaktion erfüllt, kommt nicht gross über die Intelligenz eines Insekts hinaus: Diese können auch nur gewisse Dinge im beschränkten Rahmen machen und nicht adäquat mit neuen Situationen umgehen.

Ein System, das nur Punkt 3 erfüllt, könnte man mit einem sehr introvertierten, eventuell gar autistischen Menschen, vergleichen. Dinge werden zwar - in gewisser Masse - aufgenommen, können jedoch nicht richtig verarbeitet und mit der Aussenwelt ausgetauscht werden. Eine annehmbare Kommunikation ist

¹ Diese drei Gesetze sind nicht mit den Robotergesetzen von Isaac Asimov zu verwechseln (vgl. Isaac Asimov, „I, Robot“, 1950).

aufgrund des Ausbleibens der adäquaten Reaktion nicht möglich.

Interessant aus lernpsychologischer Sicht ist in diesem Zusammenhang vor allem Punkt 2, der sich am ehesten mit folgendem Zitate des griechischen Philosophen Sokrates (469-399 v. Chr.) skizzieren: "Ich weiss, dass ich nichts weiss." Ich denke, dass dieser Punkt im Lernprozess gerne unterschätzt wird. So will man eigentlich nur lernen, wenn man sich bewusst ist, dass man etwas nicht weiss und dass die neuen Informationen einem irgendwann einen Vorteil verschaffen könnten. Wird dieser Punkt ausgelassen, kann auch der Punkt 3 nicht erfüllt werden (neue Reize werden erst nach der Fragephase aufgenommen) und somit keine Ausweitung des Wissens geschehen.

Wir kommen also nicht drum herum, der künstlichen Intelligenz ein gewisses Mass an Grundwissen mitzugeben. Es scheint utopisch, dass ein System zuerst die menschliche Sprache lernen müsste, um sich danach überhaupt Wissen ausserhalb des Bereichs der menschlichen Sprache aneignen zu können. Wie soll denn mit einem ChatBot kommuniziert werden, wenn dieser keine menschliche Sprache spricht. Wenn wir uns mit Programmcode unterhalten, ist dies ebenso eine Mitgabe an künstlichen Informationen. Einzige Lösung wäre, dass ein Bot zuerst andere Gespräche beobachtet, so wie dies auch Kleinkinder tun. Oder die ersten 100 Stunden des Betriebs der künstlichen Intelligenz findet unidirektional statt, indem der Bot die Eingaben des Benutzers speichert, ohne sinnvoll darauf zu reagieren. Früher oder später würde sich die Intelligenz einpendeln und annehmbare Dialoge wären möglich. Wenn wir darüber nachdenken, dann funktioniert das Lernen einer natürlichen Sprache nicht viel anders. Kinder brauchen ja auch mehrere Jahre, bis sie volle Sätze, mit korrekter Satzstellung und Konjunktion anwenden können.

Von der Intelligenz zum Bewusstsein

Die Intelligenz ansich ist nur ein beschränkter Teil einer umfassenden künstlichen Intelligenz. Das Bewusstsein ist quasi das Königsattribut, das darüber entscheidet, ob und inwiefern eine denkende Maschine einem Menschen ebenbürtig sein kann. Bewusstsein beschreibt die Fähigkeit, sich durch Beobachtung, Urteil und Verhalten im Kontrast zu seiner Umwelt zu erleben. Dabei ist immerwieder die Rede davon, dass man sich als Individuum versteht.

Mit den zuvor beschriebenen Mechanismen bzw.

den erweiterten Grundgesetzen des Ichs scheint es ebenfalls möglich zu sein, einer Maschine Bewusstsein "beizubringen". In einem Dialog zum Thema Bewusstsein und Tod könnte ein Benutzer seine Bedenken und Ängste vor dem Jenseits äussern. Der ChatBot nimmt diese Informationen auf und wendet sie in einem späteren Gespräch zum Thema an. Das System ist sodann in der Lage den Anschein zu erwecken, sich vor dem Ableben zu fürchten und daher als vergängliches Ich zu definieren.

Was passiert nun aber, wenn das Gespräch weitergeführt wird und der Benutzer dem System mitteilt, dass es gar kein Mensch ist und nicht in diesem Sinne sterben kann. Die Maschine wäre, da diese Weiterführung des Dialogs Neuland ist, zuerst einmal überfordert. Sie würde nachfragen, wie denn das nun gemeint sei. Früher oder später würde die Anwendung lernen, dass sie zwar ebenso vergänglich ist, aber nicht aus biologischen Gründen wie der Mensch. Dies impliziert aber nicht, dass sich nun auch nicht weiterhin die Applikation vor dem digitalen Tod fürchten kann. Genauso wie wir weiss auch der ChatBot nicht, was passiert, wenn er gelöscht wird oder die Hardware kaputt geht.

Der Überlebenstrieb von Tier und Mensch veranlasst oftmals dazu, ungeahnte Kräfte zu entwickeln. Dass dies bei unserem ChatBot nicht möglich ist, erscheint offensichtlich. Er scheint mitunter deshalb auch weiterhin unmenschlich zu bleiben. Das Argument, dass diesen Standpunkt zu wichtigen Teilen zu relativieren im Stande ist, habe ich schon zuvor genannt: Bei unserer Lösung beschäftigen wir uns lediglich mit der Intelligenz ansich. Es werden keine physikalischen und biologischen Imitationen von Menschen angestrebt. Der Computer kann also, wenn wir ihm mit der Löschung des Speichers drohen, nicht einfach aufstehen und fluchtartig wegrennen. Würden wir uns mit der Konstruktion eines Androiden befassen, wäre dies sicher möglich und wahrscheinlich eine legitime (und ebenfalls lernbare) Reaktion.

Aus Sicht der Informatik und der kognitiven Neurobiologie kann Bewusstsein auch wie folgt definiert werden: Ein System verfügt über Bewusstsein, wenn es selbständig aufgrund von Informationen aus dem Umfeld fähig ist, sich zwischen verschiedenen Verhaltensmöglichkeiten zu entscheiden, bevor eine davon umgesetzt wird. Die zuvor vorgestellte logische Gewichtung verschiedener Antworten erfüllt diese Definition.

Inwieweit kann sich künstliche Intelligenz weiterentwickeln

Wir haben gesehen, dass ein dynamisches Modell es erlaubt, dass neue Informationen verarbeitet und für weitere Interaktionen genutzt werden können. Die künstliche Intelligenz ist also in der Lage, sich in beschränktem Rahmen weiterzuentwickeln. Science-Fiction Literatur und Filme skizzieren immerwieder das Horror-Szenario, dass Maschinen mit künstlicher Intelligenz die Grenzen sprengen und einen sogenannten freien Willen entwickeln.

Ein System, wie es in dieser Arbeit vorgestellt wurde, kann dies nicht umsetzen. Durch die Hardcodierung der Grundabläufe, die wir als Instinkte bezeichnet haben, sind die Möglichkeiten der Lösung streng limitiert: Dynamik kann die Applikation nur auf den Teil der Wissensdatenbank ausüben. Die Software ist nicht in der Lage, aus diesem Gehege auszubrechen und Änderungen an den hardcodierten Instinkten vorzunehmen.

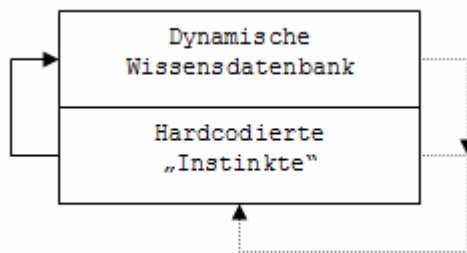


Abbildung 5: Möglichkeiten der dynamischen Manipulation

Um dies zu erreichen, müsste sie in der Lage sein, sich selber umzuprogrammieren. Dies ist kein unrealistisches Ziel, denn so könnten wir unserer Applikation durchaus die Möglichkeit gewähren, Änderungen am eigenen Programmcode vorzunehmen. Dazu müsste die Software jedoch ein grundlegendes Verständnis für das Programmieren besitzen. Ebenfalls eine Sache, die durch den Entwickler codiert zuerst werden müsste. Eine Maschine, die darauf ausgerichtet wurde, über Tastatur und Bildschirm zu kommunizieren, ist hingegen nicht plötzlich in der Lage, Änderungen am eigenen Programmcode vorzunehmen – Diese Meta-Ebene bleibt für die Software aufgrund des fehlenden „Verständnisses“ unerreichbar.

Die Sprache als dynamische Meta-Ebene

Das Herzstück unserer Kommunikation mit unserer künstlichen Intelligenz ist die geschriebene Sprache. Diese zu verstehen ist wichtigster Bestandteil des Geräts, zur Simulierung einer dem Menschen annäherbaren künstlichen Intelligenz. Wie wir schon bei der

Besprechung des Themas der erweiterten Verständnistiefe gesehen haben, ist das Verständnis für die Sprache eine Möglichkeit des Bewusstseins des Dialogs.

In einer frühen Phase verwendete ich ein Mehr an Energie, um meinem System ein Verständnis für die Sprache näher zu bringen. So versuchte ich neben der String-Analyse für die Reiz/Reaktion eine Sprachanalyse der Eingaben umzusetzen. Die Anwendung sollte Subjekt und Verb sowie etwaige Pronomen, Objekte und Partikel entdecken und entsprechend interpretieren können.

In verschiedenen Matrizen begann ich die Deklinationen, Konjunktionen, Zeitformen, usw. zu spezifizieren. Machte der Benutzer nun den Ausspruch „Mir geht es gut“, so war die Applikation in der Lage, den Standpunkt auf sich zu beziehen und daraus den Satz „Dir geht es gut“ zu formen. Indirekt bewies die Anwendung damit ein Bewusstsein: Sie konnte sich selbst von seiner Umwelt abgrenzen.

Zu Beginn machte ich es der Sache so einfach, dass ich zum Beispiel lediglich eine Auflistung der Konjunktionen von Verben in einer flachen Tabelle umsetzte:

```
haben ; habe ; hast ; hat ; haben ; habt ; ha
ben
sein ; bin ; bist ; ist ; sind ; seid ; sind
sitzen ; sitze ; sitzt ; sitzt ; sitzen ;
itzt ; sitzen
gehen ; gehe ; gehst ; geht ; gehen ; geht ;
gehen
```

Dies erforderte das Aufnehmen einer Vielzahl an Verben. Jedes von diesen musste ich durchkonjugieren und die Tabelle wuch schlagartig an. Zudem war es mir praktisch unmöglich, alle möglichen oder wenigstens gebräuchlichen Verben vorzufertigen. Ich entschied mich deshalb, mit Wortstämmen zu arbeiten und die Software die logischen Ableitungen für die Konjunktionen umsetzen zu lassen. Auf „en“ endende Verben wurden deshalb wie folgt aufgenommen:

```
en ; e ; ist ; t ; en ; t ; en
```

Danach musste ein Zuweisung alle Verben dieser Klasse erfolgen. Dabei wurden die Wortstämme wie „sitz“, „geh“, „steh“ und „lieg“ vermerkt. Begann ein Wort mit dieser Zeichenkette, so war es der Applikation sofort klar, dass es sich voraussichtlich um ein Verb handeln muss. Die Konjunktion konnte sodann anhand der Endung erkannt werden. Selbiges könnte sich auch mit den Zeitformen umsetzen

lassen, was natürlich ein enormes Mehr an Komplexität und Aufwand mit sich bringen würde.

Die deutsche Sprache gilt als eine der komplexesten und vielschichtigsten auf der ganzen Welt. Es scheint daher als besonders utopisches Unterfangen, einer künstlichen Intelligenz ein umfangendes und fehlerfreies Verständnis für diese auferlegen zu wollen. Viele Wissenschaftler postulieren deshalb die Einführung einer formalen Sprache, die eine Vereinfachung der Analyse und Gewichtung der eigentlichen Kernaussagen ermöglichen können soll. Dies ist durchaus eingangbarer Weg, wenn er auch viele neue Schwierigkeiten mit sich bringt. Neben der Entwicklung einer umfassenden und zugleich nicht zu komplexen formalen Sprache gilt es einen Konverter für diese zu erstellen. Dass bei dieser Umwandlung weitere Fehler passieren können, scheint absehbar. Für mich scheint es offensichtlich, dass die Entwicklung eines solchen formalen Systems mindestens genauso viel Zeit in Anspruch nehmen wird, wie eine künstliche Intelligenz ohne das umfassende Verständnis für die Sprache zu entwickeln.

Fazit

Intelligenz, wenn wir sie auf die drei Grundgesetze des Ichs beschränken, ist keine Zauberei. Intelligentes Handeln erscheint in diesem Kontext gar primitiv und leicht zu imitieren. Das Imitieren von Intelligenz ist ein uralter Menschheits Traum, der schon zig Mal in Angriff genommen wurde. Viele Experimente wurden eingestellt und als nicht erfolgreich abgetan. Bei vielen Vorgehen wurde aber ausser Acht gelassen, dass Intelligenz Lernen bedeutet. Lernen kostet Zeit und Zeit ist ein Faktor, den wir auf der Erde nur bedingt beeinflussen können. Entwickle ich ein Computermodell nach den in dieser Arbeit beschriebenen Mechanismen und würde ich 50 Jahre mit dem Chatten mit meinem Bot verbringen, würde dieser voraussichtlich einen Turing-Test bestehen können. Nur kein Entwickler, sei er auch noch so angefressen, wird sich hinsetzen wollen, und 50 Jahre seines Lebens mit der stumpfsinnigen Kommunikation mit einem Gerät widmen.

Die Lösung erscheint ein Kommunikationsverbund. Das Internet bietet die ideale Plattform dafür. Ein netzwerkfähiger Bot könnte tagtäglich von tausenden von Benutzern frequentiert werden, um innert wenigen Jahren die Gesprächs-Gewohnheiten dieser gelernt zu haben.

5. Kreuzworträtsel

Internet Council of Registrars	↻ 3	↘	Grosse IT-Messe	Person welche IT-Umgebung aufrecht erhält	Internet Protocol	↘	Vorname verstorbener Hacker Tron	↘	Vorgänger von Windows 2000	↘	Data Encryption Standard	Linux: Kopiert Dateien	↘
Computer messe in Basel			Versteckt geheime Datei in unzufälligen Dokument	↘						↻ 7		UNIX-Kommando equivalent zu dir unter DOS	
↘					Entfernen, um BIOS-Passwort zu resettten	Anwährte, Steuerberater TLD				Verschlüsselungs-Mechanismus für HTTP			
↘						↻ 2				Kryptographische Weiterentwicklung von Telnet			
Phreaking-Technik	Linux: Löscht den Bildschirm		Klassischer Security Scanner			Taste für Steuerzeichen				Zeilenvorschub		Advanced Program-to-Program Communication	
Gegenteil von Server		Proj. Suche nach ausserirdischem Leben	↘					Unix: Online Hilfe				↻ 5	
↘						Inet. Corp. Assigned Names and Numbers						Intrusion Prevention System	
↘		UNIX von HP				Transportprotokoll (verb.on)	Dynamische Programmiersprache fürs Web		↻ 4		Abk.: Initiale Sequenznummer	↘	
Top-Level-Domain von Schweden							DOS-Befehl Ausgabe von Verzeichnisinhalt						
↘			DOS: Benennt eine Datei um	↻ 1			Lebenszeit eines Pakets in einem Netzwerk						
Protokoll für Adressumwandlungen	Portscanner						Unix: Dateiinhalt anzeigen	Netzname eines WLAN		Unix: Verschieben einer Datei			
Unix: Löschen einer Datei						Bedieneroberfläche für OS/2	Spontanes Mehrfachzugriffsverfahren					↻ 6	
↘		JavaScript					Konkurrenzlösung zu PHP						
Unterbrechungsfreie Stromversorgung			Grafische Zeichen und Gefühlsäusserung										
↘													

Wettbewerb

Mailen Sie uns das erarbeitete Schlüsselwort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten. Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.02.2004**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

Gewinnen Sie einen Monat des [Securitytracker](#) Dienstes [pallas](#).

SECURITYTRACKER



6. Literaturverzeichnis

scip AG, scip monthly Security Summary
(smSS), Editorial, 19. März 2004

http://www.scip.ch/publikationen/smss/scip_mss-19_03_2004-1.pdf

7. 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

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Nutzen Sie unsere Dienstleistungen!

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.

Das [Errata](#) (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online.

Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)