Secorvo Security News
April 2006

Dirk Fox, Stefan Gora, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 4, 5. Jhrg. 2006
Stand 26. April 2006

ISSN 1613-4311

http://www.secorvo-security-news.de/

Inhalt

Editorial: Small World!

Wir kennen uns alle. Wenn nicht direkt, so über maximal sechs Ecken: Die These der „six degrees of separation" aus der 1929 erschienenen Kurzgeschichte *Chains* des ungarischen Schriftstellers Frigyes Karinthy (1887-1938) erlangte 38 Jahre später durch den Psychologen Stanley Milgram (1933-84) Berühmtheit, der dafür den Begriff Kleine-Welt-Phänomen prägte. Seitdem beschäftigt sie nicht nur Forscher wie Duncan J. Watts, die Karinthys These per Modell zu bestätigen versuchen, sondern wurde erfolgreich in Geschäftsmodelle (wie z. B. Online-Kontaktnetzwerke) umgesetzt.

Bewiesen ist Karinthys These bisher nicht, widerlegt werden konnte sie allerdings auch nicht. Selbst in OpenBC, mit einer Million Benutzern eine der erfolgreichsten Online-Kontaktbörsen, lässt sich auch zu Neu-Usern keine Kontaktkette finden, die länger ist als sechs.

Auch Vertrauensnetze wie das „Web of Trust" von PGP profitieren von kurzen Vertrauensketten – je kürzer, desto größer das Vertrauen in die Identität eines fremden Schlüsselinhabers. Voraussetzung für diese enge Vermaschung ist dabei die Verknüpfung der Beziehungsdaten: Aus mehr Beziehungen resultiert eine kürzere Kette – und damit mehr Vertrauen.

Sollten wir also mehr Beziehungswissen preisgeben, um mehr Vertrauen zu erreichen? Das zu glauben wäre ein typischer Naturalistischer Fehlschluss – ein unzulässiges Ableiten von Soll- aus Ist-Zuständen. Denn je enger wir „zusammenrücken", desto wichtiger wird der Schutz der Privatsphäre – sofern wir eine erhalten wollen.

Auch in der Online-Enzyklopädie Wikipedia wirkt das Small-World-Phänomen („Six degrees of Wikipedia"): „Kleine-Welt-Phänomen" und „Naturalistischer Fehlschluss" sind über fünf Links verbunden (Soziale Netzwerke – Soziologie – Philosophie – Sprachphilosophie – G. E. Moore). Bis zum „Datenschutz" ist die Kette allerdings einen Klick länger (Soziale Netzwerke – Herrschaft – Gesetze – Grundgesetz – Grundrechte – Informationelle Selbstbestimmung).

1 Security News

1.1 GnuPG legt nach

Am 03.04.2006 ist eine neue Version der freien Krypto-Software GnuPG erschienen. Während frühere Versionen in erster Linie Sicherheitslücken bereinigten, enthält Version 1.4.3 etliche interessante neue Features: Neben dem deutlich verbesserten Management von GPG-Schlüsseln unterstützt GnuPG nun einige der DNSSEC-Erweiterungen direkt. Dabei geht es in erster Linie darum, kryptographisches Schlüsselmaterial sowie Zertifikate im DNS speichern und von dort abrufen zu können.

GnuPG kann jetzt auf diese Erweiterungen zugreifen. Interessant ist dies deshalb, weil DNSSEC zwar schon seit Jahren „kurz vor der Einführung steht“ (vgl. SSN 05/2004, SSN 04/2005), bis heute aber nur wenig bis gar kein Gebrauch davon gemacht wird – ein Grund dafür war die mangelnde DNSSEC-Unterstützung in den Anwendungen.

1.2 ... und keiner merkt's

Wie erst am 31.03.2006 in einem Report veröffentlicht, waren die Root-Nameserver im Februar dieses Jahres wieder einmal Ziel einer großflächigen Denial-of-Service-Attacke. Die Angreifer setzten Bot-Netze ein, um die DNS-Server mit übergroßen Paketen zu beschäftigen.

Pikanterweise versuchten die Angreifer eine recht neue Erweiterung des DNS-Protokolls auszunutzen: EDNS0 wurde erst im Rahmen der DNSSEC-Aktivitäten spezifiziert und implementiert, um die ehemals geltende Größenbeschränkung von 512 Bytes pro DNS-Paket aufzuheben, damit beispielsweise kryptographische Schlüssel via DNS transportiert werden können (s.o.).

Wie schon bei früheren Angriffen wirkte die Attacke nur bei schlecht konfigurierten Nameservern. Geholfen hätte auch diesmal die korrekte Konfiguration der Nameserver gemäß längst bekannten Best-Practice-Methoden – nicht besondere Schutzmechanismen à la DNSSEC. Interessanterweise hat jedoch auch diesen Angriff kaum ein Endbenutzer wahrgenommen...

1.3 IPv6-Werkzeugkasten

Seit der cansecwest/core06 ist das dort Anfang April 2006 vorgestellte „IPv6 Attack Toolkit“ von THC/VH auch für die Allgemeinheit zur praktischen Verwendung verfügbar. Die darin enthaltenen 12 Spezialwerkzeuge und die zu Grunde liegende „IPv6 packet factory library“ demonstrieren u. a. Schwachstellen in IPv6, die auf Angriffsstrategien wie Denial-of-Service und Man-in-the-Middle beruhen. Die Packet Library selbst sowie der verfügbare Sourcecode (derzeit noch auf Linux beschränkt) ermöglichen sowohl die einfache Erstellung weiterer „Werkzeuge“, als auch die Änderung der Paketsignaturen, um Intrusion Detection Systemen zu entwischen.

Mit diesem Werkzeugkoffer existiert erstmals eine abgestimmte Tool-Sammlung für Netzwerksicherheitsanalysen von IPv4 mit parallel zugelassenem IPv6.

1.4 VM Based Rootkits

Eine neue Variante von Rootkits wurde von Forschern der Michigan University und Microsoft Research vorgestellt: Durch die Kombination von Rootkits mit der Technik virtueller Maschinen entstehen perfide aber auch technisch anspruchsvolle Angriffsmöglichkeiten. Die im Rahmen des Projekts „SubVirt“ auf Basis von VirtualPC und VMware entwickelten Tools übernehmen dabei komplett die angegriffenen Systeme unter Windows XP oder Linux und emulieren das ursprüngliche Betriebssystem innerhalb einer virtuellen Maschine. Eine zweite virtuelle Maschine kann für beliebige Angriffszwecke wie beispielsweise den Betrieb eines Phishing Webservers verwendet werden.

Das Fatale an dieser Technik ist, dass die Übernahme für den Benutzer nicht erkennbar ist: Da die Benutzermaschine durch die VM-Umgebung kontrolliert wird, fanden die Forscher in ihren Untersuchungen lediglich den deutlich verlängerten Bootvorgang und

eine verminderte 3D-Leistung als Indizien. Da solche Virtual Machine Based Rootkits (VMBRs) sogar Shutdown-Prozesse emulieren und das System in standby versetzen, ist selbst ein Neustart des Benutzersystems unter Kontrolle des Rootkits. Nur wenn das System wirklich „aus“ ist, kann von einem alternativen Medium gebootet und das Rootkit festgestellt werden.

Die Ergebnisse der Forschungen und weitere Schutzmaßnahmen sind im Paper „SubVirt: Implementing malware with virtual machines" zusammengefasst, welches für das diesjährige IEEE Symposium on Security and Privacy eingereicht wurde.

1.5 Selbsthilfe-Ecke

Gegen Spam gibt es eine Reihe von technischen Gegenmaßnamen wie Spamfilter und Greylisting. Eine der wirksamsten Methoden ist aber immer noch, Vorsicht bei der Preisgabe oder Weitergabe seiner E-Mail-Adresse walten zu lassen.

Aber was tun, wenn man sich Informationen zusenden lassen oder auf einer Website registrieren will? Ein Weg ist die Nutzung von Einmal- oder Wegwerf-E-Mail-Adressen, vorgeschlagen von Stefan Kelm auf dem Anti-Spam-Symposium 2003. Dabei helfen Angebote wie Spamgourmet: Dort können temporäre E-Mail-Adressen eingerichtet werden, die eingehende E-Mails an die „echte“ eigene E-Mail-Adresse weiterleiten. Nach einer zuvor festgelegten Zahl eingegangener E-Mails wird die Adresse vom Anbieter automatisch gelöscht. Dem Anbieter muss man allerdings vertrauen, dass er die echten Adressen keinem Dritten preisgibt.

1.6 Kapitulation

Das Bundeskabinett hat am 25.04.2006 einen Gesetzentwurf aus 16 Einzelmaßnahmen zum „Abbau bürokratischer Hemmnisse insbesondere der mittelständischen Wirtschaft“ verabschiedet. Darunter: Die Anhebung des Schwellwerts für die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten. Die soll zukünftig nur noch bestehen, wenn mindestens 10 (und nicht wie bisher fünf) Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. Schon am 22.07. 2005 hatten die Länder Hessen und Niedersachsen einen Gesetzentwurf im Bundesrat eingebracht, der das Quorum auf mindestens 20 Arbeitnehmer anheben will; am 23.09.2005 winkte der Bundesrat diesen Entwurf durch. Die Festlegung des Kabinetts auf ein Quorum von 10 riecht verdächtig nach Formelkompromiss – eine inhaltliche Begründung gibt es nicht.

Tatsächlich wirkt die vermeintliche Entbürokratisierungsmaßnahme wie eine Kapitulation vor dem faktischen Vollzugsdefizit in kleinen und Kleinstunternehmen: Die wenigsten kommen bisher der seit 1978 bestehenden Pflicht zur Berufung eines betrieblichen Datenschutzbeauftragten nach, und selbst das oft nur pro forma.

Allerdings war es noch nie ein Ausdruck besonderer Weisheit, bedauernswerte Ist-Zustände zu Soll-Zuständen zu erheben (siehe Editorial). Zwar würden durch diese Regelung über 90 % der deutschen Unternehmen von der Verpflichtung befreit – so viele der insgesamt knapp drei Millionen Betriebe beschäftigen maximal 10 Mitarbeiter. Bestehen bleiben jedoch alle anderen Verpflichtungen: die Auskunftspflichten gegenüber den Betroffenen, die Festlegung und Einhaltung von Löschfristen, die Prüfung der Rechtmäßigkeit und Ordnungsmäßigkeit der Verarbeitung, die Schulung und Verpflichtung der Mitarbeiter auf das Datengeheimnis sowie eine gesetzmäßige Vertragsgestaltung bei Auftragsdatenverarbeitung und Übermittlung in Drittländer. Wer aber wird zukünftig in diesen Unternehmen die Sachkunde besitzen, für die Einhaltung des BDSG zu sorgen?

Bedenklich ist, dass hier mit dem Argument der Entbürokratisierung der Schutz des zentralen Grundrechts der freien Entfaltung der Persönlichkeit geschwächt wird. Denn außer Frage steht, dass die Konstruktion des betrieblichen Datenschutzbeauftragten in Deutschland erheblich zum international vergleichsweise hohen Schutz personenbezogener Daten beiträgt.

2 Secorvo News

2.1 Secorvo College aktuell

Gleich zwei neue Seminare stehen im Mai auf der Agenda von Secorvo College:

- IT-Sicherheitsaudits in der Praxis führt am **09.-10.05.2006** in die Grundlagen aussagefähiger Sicherheitsanalysen ein – von der Planung über die technische und organisatorische Prüfung bis zu Tools, rechtlichen Rahmenbedingungen und Praxiserfahrungen.
- IT-Outsourcing sicher gestalten trägt der wachsenden Bedeutung von Sicherheitsfragen bei der Auslagerung von IT-Prozessen Rechnung. Rechtsfragen, die Gestaltung von SLAs und die Einbindung in das Sicherheitsmanagement stehen im Zentrum des eintägigen Seminars am **11.05.2006**.

Programme und Online-Anmeldung:
www.secorvo.de/college

2.2 Security Awareness

Am 02.-03.05.2006 findet das inzwischen vierte „Security Awareness Symposium“ statt – mit Praxisberichten von Areva NP, DAK, SwissRe und T-Systems und einem intensiven Erfahrungsaustausch. Für Kurzentschlossene empfehlen wir die Online-Anmeldung – es gibt nur noch wenige freie Plätze.

2.3 Honeypots betreiben

Honeypots und Honeynets sind bereits seit einiger Zeit als effektive Sicherheitskomponente bekannt; dennoch waren viele Unternehmen sehr zurückhaltend, wenn es um den Aufbau entsprechender Honeypot-Umgebungen innerhalb der eigenen Infrastruktur ging. Dies scheint sich jetzt zu ändern: immer mehr Nachfragen haben uns veranlasst, die von Secorvo bereits seit einiger Zeit angebotenen Dienstleistungen in diesem Bereich in einem Leistungsangebot zusammen zu stellen und zu veröffentlichen.

2.4 Veranstaltungshinweise

Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
23.05.	„Wem die Stunde schlägt“ (amec spie/Lampertz, Rust)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
30.05. - 01.06.	Web-Application Security (Secorvo College, Karlsruhe)
Juni 2006	
06.-09.06.	ETRICS 2006 (Univ. Freiburg)
20.-22.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
21.-22.06.	Midvision 2006 (Karlsruher Messe)
25.-30.06.	Annual FIRST Conference 2006 (FIRST, Baltimore/US)
27.-28.06.	Lotus Notes Security (Secorvo College, Karlsruhe)
29.06.	Lotus Notes Security – advanced (Secorvo College, Karlsruhe)
Juli 2006	
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)

Aktuelle Veranstaltungsübersicht:
http://www.veranstaltungen-it-sicherheit.de/

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14, D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)
Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de