secorvo
security consulting

Secorvo Security News

Dezember 2007

Editorial: Ganz einfach

Alles Große und Edle ist einfacher Art.
Gottfried Keller (1819-1890)

Die Komplexität hat uns im Griff. Sowohl im Großen (Termine, Aufgaben) als auch im Detail (Umsetzungsprobleme, Prozesse, Tools). Schleichend haben wir die Übersicht der Vielfalt geopfert. Der Trend zum Komplexen verursacht Mehraufwände, Ärger und Verzögerungen, die von keinem Controller gemessen werden – und gefährdet die Sicherheit unserer Systeme. Denn Komplexität erhöht die Anfälligkeit für Fehler (Software, Bedienung, Hardware), erschwert zugleich die Kontrolle und verbaut den Blick auf das Wesentliche: Sind Prioritäten ereignisgetrieben und vernebeln diffuse Ziele die Aufgaben, geht leicht der Überblick verloren.

Die Erkenntnis, dass Konzentration auf das Wesentliche die Effektivität steigert, ist ebenso banal wie bekannt – aber selten beachtet. Doch Vorsicht: Einfachheit ist harte Arbeit. Sie erfordert drei Dinge:

- **Klarheit**: Formulieren Sie Sicherheitsziele und Regeln verständlich, nachvollziehbar und eindeutig – und vor allem: im Kontext Ihrer Unternehmensziele. Jede Policy und jede Maßnahme sollte sich daraus mit „gesundem Menschenverstand" ableiten lassen.
- **Konsequenz**: Sorgen Sie für die Umsetzung Ihrer Basis-Sicherheitsmaßnahmen – wie personalisierte Accounts, Mindestanforderungen an die Passwortqualität, Unterbindung von Passwortweitergaben, „Need-to-Know"-Prinzip für Administratorrechte, Schutz mobiler Systeme. Damit schließen Sie die „Löcher im Zaun" und erzielen die mit Abstand beste Wirkung.
- **Verzicht**: Verhindern Sie nebulöse Floskeln, vermeidbare Regelungen, nicht konsequent umsetzbare Maßnahmen. Sie gewinnen Sicherheit, wenn Vereinfachung die Umsetzung erleichtert.

Ingenieure lieben es, Komplexität zu konstruieren.
Die Konstruktion von Einfachheit ist um Einiges schwieriger. Shai Agassi

Inhalt

secorvo
security consulting

Security News

Wireless Hacking

Am 30.11.2007 veröffentlichte die Schweizer Firma Dreamlab Technologies ein Whitepaper, in dem sie Details der Verschlüsselung in Microsofts Funktastaturen offen legt. So werden die Tastatureingaben lediglich durch einen einfachen XOR-Mechanismus mit einem ein Byte langen Zufallswert kryptiert (Vigenère-Chiffre, vor 151 Jahren von Charles Babbage gebrochen); dieser Zufalls-„Schlüssel" wird nach einem „Connect" der Tastatur im Klartext an den Receiver geschickt. Da es nur 256 mögliche Schlüssel gibt, lohnt es nicht, den Wert abzufangen – schon nach wenigen Tastatureingaben (20-50) kann die Zufallszahl bestimmt werden. Manchmal lohnt es, sich mit seiner eigenen Geschichte zu beschäftigen: Mit demselben „Verschlüsselungsmechanismus" hatte Microsoft sich schon bei Office 95 blamiert.

Immerhin gibt es zahlreiche Funktastaturen am Markt, die selbst auf eine solche Verschleierung verzichten. Daher sind nach Geheimschutzhandbuch des BMWi für IT-Systeme, mit denen Verschlusssachen verarbeitet werden, gemäß Abschnitt 6.11.2 (1) Funktastaturen nicht zugelassen.

Mobile Bots

Das am 27.11.2007 von der ENISA publizierte Positionspapier „Botnets - The Silent Threat" liefert eine aktuelle Analyse der Botnet-Szene. Die statistischen Daten stammen überwiegend aus dem ATLAS-System (SSN 02/2007). Danach werden 65% der „Zombie"-Systeme über Browser-Exploits infiziert.

Nach Überzeugung der ENISA sind Botnetze (mit insgesamt ca. 6 Mio. Bots) ein Werkzeug der organisierten Kriminalität. Sie stuft sie aufgrund der technischen Ausgereiftheit und andauernden Weiterentwicklung als mittelfristig ernsthafte Gefährdung der globalen Netzwerkinfrastruktur ein. Insbesondere mobile, vernetzte Endgeräte mit ständigem Netzzugang dürften zukünftig eine bevorzugte Zielplattform für Botnetze darstellen (s. a. iPhone out of Jail, SSN 10/2007).

Der Kern des Problems, die Unsicherheit von Programmen und Betriebssystemen, wird in dem Papier zwar angesprochen, mündet jedoch in der wenig spektakulären Forderung, „*Vendors should continuously improve the security of their products*". Statt der Hersteller (Produkthaftung) nimmt die ENISA die ISPs in die Pflicht: Sie sollen Botnetz-E-Mails erkennen und blockieren.

Selbst-Inspektion

Nach einer einjährigen Beta-Phase hat das dänische Unternehmen Secunia am 18.12.2007 Release 1 des Personal Software Inspectors (PSI) freigegeben. Das für Privatnutzer lizenzfrei nutzbare Tool überprüft Windows-Betriebssysteme und zahlreiche installierte Standard-Anwendungen, ob technische Schwachstellen existieren, Softwareversionen veraltet sind oder Programme nicht mehr vom Hersteller unterstützt werden. PSI erkennt mehr als 4.700 Programm(versionen) anhand einer eigenen Signatur-Datenbank. Praktischerweise liefert das Analyseergebnis auch die direkten Download-Links der erforderlichen Sicherheits-Updates. Ein wertvolles Hilfsmittel, will man sich durch konsequentes Securitypatch-Management vor Bedrohungen schützen, die von bekannten Fehlern installierter Programme und Betriebssysteme ausgehen.

EU-Signatur-Studien

Pünktlich zur besinnlichen Adventszeit legte die EU-Kommission zwei Studien zum Thema elektronische Signaturen auf den virtuellen Gabentisch. Sie sind „Nachfolger" der Study on legal and market aspects of electronic signatures (2003), an der auch Secorvo mitwirkte und die der Kommission eine Reihe von Empfehlungen mit auf den Weg gab (vgl. SSN 10/2003). Die Studien untersuchen erneut den Stand der Umsetzung der EU-Signaturrichtlinie in ausgewählten Bereichen. Beide Studien wurden am 12.12.2007 in Brüssel der Öffentlichkeit vorgestellt.

Die am 22.11.2007 fertig gestellte Study on the standardisation aspects of eSignature analysiert die zahlreichen Initiativen en Detail, die entweder innerhalb oder außerhalb offizieller Gremien die Standardisierung im Bereich Signaturen voran getrieben haben. Dabei werden die existierenden Standards sehr unterschiedlich bewertet (von „zu vage" bis „zu detailliert"); Probleme sehen die Autoren vor allem bei der Veröffentlichung von Standards im Amtsblatt der Europäischen Union. Zur Verbesserung werden eine Reihe von teilweise sehr pragmatischen Maßnahmen empfohlen.

Eine gänzlich andere Fragestellung untersucht die – bislang nur als Vorstudie publizierte – Study on mutual recognition of eSignatures for eGovernment applications. Sie analysiert wie die gegenseitige Anerkennung elektronischer Signaturen im E-Government innerhalb Europas verbessert werden kann, und richtet zahlreiche Empfehlungen an die EU (insbesondere die Einrichtung einer „European Generic Validation Authority"), die Mitgliedsstaaten sowie an die für PKI-Anwendungen Verantwortlichen. Man darf gespannt sein, wie viele der Empfehlungen diesmal umgesetzt werden.

BCM bald zertifizierbar

Im November 2006 wurde der Empfehlungsstandard BS 25999-1:2006 „Business continuity management. Code of Practice“ veröffentlicht. Ein Jahr später erschien nun dessen Pendant, der Anforderungsstandard BS 25999-2:2007 „Specification for business continuity management“ des englischen BSI (British Standards Institute), der die Grundlage für den Nachweis eines BCM-Systems bilden kann.

Die Ähnlichkeiten zum ISO/IEC 27001:2005, der aus dem BS 7799-2:2002 hervorging, sind nicht zufällig. Auch der BCM-Standard setzt auf das bewährte PDCA-Modell (Plan-Do-Check-Act) als Grundlage eines „lebendigen“ Management-Systems. Generell bewegt sich der nur 28seitige Standard auf einem abstrakten Niveau und enthält im Gegensatz zum ISO/IEC 27001:2005 keinen Katalog mit konkreten Umsetzungsmaßnahmen.

Damit steht nur noch die Veröffentlichung des neuen BSI-Standards 100-4 zum Thema Notfallmanagement aus. Darin wird der Praktiker zweifellos konkretere Hilfestellungen finden.

Sicherheitspreis 2008

Zum zweiten Mal hat die Horst-Görtz-Stiftung des Utimaco-Gründers am 08.12.2007 den mit insgesamt 200.000 Euro dotierten Deutschen IT-Sicherheitspreis ausgelobt. Prämiert werden innovative Konzepte und Lösungen aus den Bereichen Kryptografie, System- und Netzwerksicherheit. Eine Bewerbung ist schriftlich bis 18.02.2008, online bis 28.02.2008 möglich. Die Preisverleihung erfolgt im Oktober 2008 in Darmstadt.

Eichhörnchen mit Backdoor

Am 13.12.2007 entdeckten die Entwickler des beliebten Open-Source Webmailers SquirrelMail, dass die MD5-Summen der veröffentlichten Software-Pakete von Version 1.4.12 nicht stimmten. Tatsächlich konnte eine nachträgliche Veränderung des Codes festgestellt werden, durch die die Ausführung beliebigen Programmcodes – und damit bösartige Angriffe – ermöglicht wurden. Wir raten daher dringend zum Update auf die neueste Version 1.4.13. Und: Vor der Installation von öffentlich zugänglicher Software sollte immer die Integrität geprüft werden! Das kleine Tool Hashtab (Version 2.07 vom 13.12.2007) vereinfacht dies für Dateien unter Windows erheblich. Es unterstützt zehn auswählbare Hash-Algorithmen (u. a. RIPEMD, MD5 und SHA-1).

Trojaner 2.0

Der Internet-Sicherheitsspezialist finjan hat am 10.12.2007 seinen Web Security Trends Report (Q4 2007) veröffentlicht. Interessantester Schwerpunkt dieses Berichts ist die Prognose für die Entwicklung der Steuerung von Trojanern auf infizierten PCs. Die traditionellen Wege – Nutzung von IRC und IRC über HTTP als dedizierte Kommunikationszentren – erlaubte ein (mühseliges) Blacklisting dieser Dienste.

Der finjan-Report sagt voraus, dass mit der Verbreitung von Web 2.0-Techniken diese vermehrt auch zur Steuerung von infizierten Drohnen genutzt werden. Die Übertragung von Daten zum infizierten Rechner erfolge per RSS-Feed, während als Rückkanal Blog-Services oder offene Web 2.0-Plattformen genutzt würden. Moderne verteilte APIs verschiedener Plattformen erleichterten diesen Ansatz. Dies würde eine effektive Verteidigung signifikant erschweren, da der bösartige Datenverkehr transparent in zulässige Datenströme eingeflochten und somit kaum noch zu filtern sein würde. Perimeter-Schutz hilft da nicht weiter: Die Nutzung wirksamer Sicherheitsmechanismen in Applikationen gewönne weiter an Bedeutung.

Erratum

Anders als in den SSN 11/2007 behauptet wurde in der Neufassung des BSI-„Leitfadens IT-Sicherheit“ keineswegs der Begriff „Härten (...) in der IT-Sicherheit“ gestrichen. Wir bitten um Entschuldigung. Über die Feiertage üben wir Lesen. Versprochen.

Secorvo News

Secorvo College aktuell

Noch nie haben so viele Teilnehmer unsere Seminare besucht wie 2007 – sogar Zusatztermine mussten wir kurzfristig einschieben. Stolz machen uns vor allem die hervorragenden Bewertungen und die zahlreichen Empfehlungen aus berufenem Mund wie diese: „*Secorvo überzeugt durch exzellente Fachkompetenz, den Bezug von IT-Sicherheit zur Wirtschaftlichkeit, die Professionalität der Dozenten und nicht zuletzt die hervorragende Organisation der Schulung. Ich habe Secorvo weiterempfohlen.*“ (Markus Hieb, Roche Diagnostics GmbH).

Wir danken Ihnen für Ihr Vertrauen und freuen uns auf ein Wiedersehen in 2008 auf einem unserer zahlreichen Seminare.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Dezember 2007	
24.12.	Heiligabend
27.-30.12.	The 24th Chaos Communication Congress (24C3) (Chaos Computer Club, Berlin)
Januar 2008	
16.-18.01.	Omicard 2008 (inTIME, Berlin)
Februar 2008	
05.-06.02.	18. SmartCard Workshop (Fraunhofer, Darmstadt)
10.-13.02.	Fast Software Encryption Workshop (FSE 08) (IACR, Lausanne/CH)
11.-14.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-14.02.	15. DFN CERT & PCA Workshop - Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
19.-20.02.	Identity Management Symposium 2008 (vps & Secorvo, Karlsruhe)
25.-29.02.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
März 2008	
09.-12.03.	11. International Workshop on Practice and Theory in Public Key Cryptography (IACR, Barcelona/ES)
11.-14.03.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)
19.-21.03.	5. Theory of Cryptography Conference (TCC 2008) (IACR, New York/US)

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an
redaktion-security-news@secorvo.de