secorvo
security consulting

Secorvo Security News

April 2009

Editorial: Kuckucks-Eier

Abgesehen von gesetzlichen Pflichten ist die Reduktion operationeller Risiken die einzige vertretbare Begründung für Investitionen in den Schutz sensibler Daten und Information.

Als Existenznachweis für solche Risiken erfreuen sich die Ergebnisse von Studien und Befragungen großer Beliebtheit – besonders, wenn Teilergebnisse die eigenen Argumente untermauern. Tatsächlich aber besitzen veröffentlichte Studien fast ausnahmslos dieselben Schwächen: die Zahl der Befragten ist gering, die Fragen unscharf und interpretationsbedürftig, was wiederum die Aussagekraft der Antworten schwächt, und die Auswertung ist oberflächlich bis tendenziös. Nicht zuletzt mündet die Auswahl der Befragten (überwiegend selbst IT-Sicherheitsbeauftragte) oft in der gegenseitigen Bestätigung gemeinsam geteilter Vorurteile.

Eindrucksvoll belegt dies der am 14.04.2009 publizierte 2009 Data Breach Investigations Report von Verizon, für den 90 Sicherheitsvorfälle systematisch analysiert wurden. Dabei zeigte sich: Die meisten Vorfälle hatten mehrere Ursachen und ließen sich nicht in die beliebten simplen Verursacherkategorien „Insider“ oder „Externer“ einordnen. Zahlreiche Hacking-Attacken wären ohne die Ahnungslosigkeit oder den Leichtsinn von Mitarbeitern nicht erfolgreich. Und: Die absolute Zahl bestimmter Angriffe und auch deren prozentualer Anteil sagt wenig über das tatsächliche Risiko, denn das wird wesentlich von dem durch den Angriff verursachten Schaden bestimmt.

Wer bei der Steuerung seiner Investitionen in die Informationssicherheit auf zweifelhafte Studienergebnisse setzt, lässt sich fremde Eier ins Nest legen. Belastbare Hinweise auf das tatsächliche eigene Risiko ergeben sich nur bei vorurteilsfreier und differenzierter Analyse und Bewertung der eigenen Schwachstellen.

Wer dennoch aus Scheu vor dem Ruf des „Propheten im eigenen Lande“ zu Studien greifen möchte, sollte es wenigstens mit Sir Winston Churchill halten: „Ich glaube nur der Statistik, die ich selbst gefälscht habe.“ Sofern das Zitat ihm nicht untergeschoben wurde.

Inhalt

secorvo
security consulting

Security News

Signatur-Ei

Die Prüfung elektronischer Signaturen ist ein typisches Henne-Ei-Problem: Um eine Signatur zu prüfen, muss man auch das Zertifikat des Signierenden prüfen, das die Signatur einer ausstellenden Certification Authority (CA) trägt, die es wiederum zu prüfen gilt. Das Ganze muss man so lange fortsetzen, bis man am Ende der Kette bei einer vertrauenswürdigen, bekannten Henne (sprich: Root CA) bzw. deren Ei (sprich: Stammzertifikat) angekommen ist.

Doch damit nicht genug: Für jedes dieser Zertifikate im Eierkorb will auch noch validiert sein, ob es nicht bereits vor Erreichen seines aufgedruckten Haltbarkeitsendes als verdorben erkannt wurde. Dazu wird eine Sperrliste oder Online-Statusauskunft zu Rate gezogen, die – der Leser ahnt es sicher schon – ihrerseits signiert ist und über eine Kette von Zertifikaten geprüft werden muss, für die auch jeweils der Sperrstatus zu validieren ist – und so weiter und so fort …

Und wie man beim Eierkauf schaut, ob die Eier auch keinen Knacks in der Schale haben, so ist zu prüfen, ob alle Signaturen mit sicheren Algorithmen und Schlüssellängen erstellt wurden. Weil aber bei letzteren nur besonders feine Nasen erkennen, wann sie faulig zu duften beginnen, veröffentlicht die Bundesnetzagentur (BNetzA) jährlich im Bundesanzeiger eine aktuelle Liste aller Algorithmen der Hkl. A (zuletzt am 27.01.2009).

Am 06.03.2009 nun wies die BNetzA darauf hin, dass einer vermeintlich qualifizierten Signatur ein gegenüber § 371a ZPO verminderter Beweiswert zukommt, wenn bei der Prüfung des ganzen Hühnerstalls voller Hennen und Eier ein fauler Algorithmus entdeckt wird, der nicht rechtzeitig durch eine neue Eierschale (sprich: Übersignatur) gekittet wurde. Damit ergibt sich als siebte Klasse elektronischer Signaturen (vgl. SSN 02/2003) die „qualifizierte Signatur Hkl. B“ – mit abgelaufener Mindesthaltbarkeit. Vielleicht sollten potenzielle Anwender schon einmal beim Eierkauf üben und die Augen für das Kleingedruckte offen halten.

Konjunktur-Ei

Die Bundesregierung verteilt gerade Ostergeschenke in Gestalt von Konjunkturpaketen. Darunter finden sich 30 Millionen Eier, die gemäß der Antwort auf eine Kleine Anfrage der FDP-Bundestagsfraktion vom 25.03.2009 zur Steigerung der IT-Sicherheit verwendet werden sollen.

So ist geplant, von Anfang 2010 an über eine Million „IT-Sicherheitskits“ in Form von Kartenlesern und Software zur Nutzung der optionalen Authentifikations- und Signaturfunktionen der elektronischen Gesundheitskarte und des künftigen elektronischen Personalausweises zu verschenken – bevorzugt an die Teilnehmer des geplanten Anwendungstests (vgl. SSN 12/2008). Wie praktisch: Ein Softwarepaket zur Installation auf Privatrechnern – „from the people who brought you the Bundestrojaner“. Wer wird sich wohl so ein Ei ins eigene Nest legen?

RZ-Ei

Die gleichzeitige Gewährleistung von Vertraulichkeit und Verfügbarkeit gespeicherter Daten ist oft ähnlich schwierig, wie ein Omelette zuzubereiten, ohne dabei die Eier zu zerschlagen – „wasch' mich, aber mach' mich nicht nass“. Ein besonders hübsches Beispiel für diese Quadratur des Eis ist die von der israelischen Firma Axxana vermarktete Daten-Black-Box (am 30.03.3009 von Gartner in den Rang eines „Cool Vendor in Storage Technology and Systems“ erhoben). Darin sollen die Daten eines Rechenzentrums ähnlich geschützt sein wie ein rohes Ei in der richtigen Verpackung.

Damit man dieses „Daten-Ei“ selbst in einem eingestürzten Gebäude schnell finden kann, hat es einen eingebauten Peilsender. Und will man auf die wertvollen Daten nicht warten, bis alle Trümmer beiseite geräumt sind, lässt sich über eine Fernbedienung das drahtlose Netzwerk der Box aktivieren. Fragt sich nur, woran die Box erkennen kann, dass sie unter Trümmern begraben liegt – und nicht die Aufmerksamkeit eines nicht-autorisierten Eiersuchers auf sich gezogen hat.

Entwickler-Ei

„Easter Eggs“ werden verborgene Funktionen in Programmen genannt, mit denen sich die Entwickler ein „Denkmal“ gesetzt haben. Alte Bekannte sind der Flugsimulator in Microsoft Excel oder Space Invadors in Word. Aber auch in zahlreichen aktuellen Programmversionen lassen sich „Easter Eggs“ finden. Oft sind sie im Umfeld der Versions- und Copyright-Angaben verborgen, und meist muss man Insider-Kenntnisse haben, um sie zu finden – wie die „about:robots“-Seite in Firefox. Eine der bekanntesten Sammlungen solcher Easter Eggs findet sich auf eeggs.com.

Derartige Eier sollten allerdings auch daran erinnern, dass sich in jedem Programm unbekannte Funktionen verbergen können – auch solche, die nicht einmal vom Programmierer intendiert waren. Und unter diesen Eiern kann das eine oder andere faul sein. Merke: Die Axt im Haus erspart den Zimmermann – und die Backdoor im Programm einen mühsamen Hackerangriff.

Backbone-Ei

Auch im Backbone-Bereich wurden erst kürzlich einige Eier gefunden, u. a. von Enno Rey und Daniel Mende, die diese am 16.04.2009 auf der Blackhat Europe vorstellten. In ihrer Präsentation zeigten sie, wie man die durch MD5 gesicherten Signaturen von BGP (Border Gateway Protocol) kompromittieren kann, zum Beispiel mit dem von ihnen entwickelten Tool bgp_md5crack. Außerdem stellten die Autoren fest, dass man die Vertrauensanker von MPLS-VPNs kritisch prüfen sollte.

Auch wenn die Angriffsmöglichkeiten durch Tools wie mpls_redirect entsprechende Zugangsmöglichkeiten im Core-Bereich voraussetzen, weist der Vortrag nach, dass der Zugang alleine ausreichen kann, um den Verkehr umzuleiten. Die unterhaltsamen Folien können von der Webseite der Autoren herunter geladen werden.

Ankündigungs-Ei

Am 20.03.2009 veröffentlichte das US Department of Homeland Security einen Bericht über eine Überprüfung der Sicherheitssysteme an verschiedenen amerikanischen Flughäfen, die im Vorfeld bei der TSA intern per E-Mail angekündigt worden war. Die Darlegung von Details der geplanten Tests in dieser E-Mail musste zwangsläufig zur Nutzlosigkeit der verdeckt geplanten Überprüfung führen.

Als Aprilscherz wäre der Bericht vielleicht lustig zu lesen; tatsächlich muss er als Lehrstück verstanden werden, wie Tests und Audits gerade nicht durchgeführt werden sollten.

Datenbank-Ei

Einen ganzen Korb fauler Eier präsentierte Oracle am 14.04.2009 in seinem vierteljährlichen Critical Patch Update Advisory (letzte Aktualisierung vom 22.04.2009): Insgesamt 43 kritische Sicherheitslücken stopfen die Patches. Darunter finden sich zwei, die durch Fernzugriff auf eine Oracle-Datenbank ohne Authentisierung ausgenutzt werden können, und zwei weitere, die auf dieselbe Weise Peoplesoft Enterprise betreffen – in vielen Unternehmen mit amerikanischen Müttern das führende HR-System.

Betroffene Unternehmen sollten umgehend patchen – und die Datenschutzbeauftragten kritisch nachfragen.

Wurm-Ei

Am 22.04.2009 entdeckte Manh Dzung, Senior Malware Analyst beim vietnamesischen Unternehmen Bach Khoa Internetwork Security in Hanoi, einen Wurm, der Captchas von Google Mail löst – und so in der Lage ist, anonym eine beliebige Anzahl von E-Mail-Konten anzulegen. Die Analyse der Captchas übernimmt ein auf einem kanadischen Server beheimateter Dienst, an den der Wurm die Captcha-Grafik per E-Mail sendet.

Den erhofften Schutz vor automatisierten Angriffen bieten Captchas (vgl. SSN 2/2008) nicht mehr – die Tricks von Würmern und Trojanern kombiniert mit der Leistungsfähigkeit heutiger Analyse-Algorithmen macht eine verlässliche Unterscheidung von Mensch und Maschine praktisch unmöglich.

Secorvo News

Secorvo College aktuell

Den Sommer beginnen wir mit der nächsten Gelegenheit zur Zertifizierung Ihrer persönlichen Qualifikation: Das zweite T.I.S.P.-Seminar dieses Jahres findet vom 22. bis 27.06.2009 statt – Zertifikatsprüfung inklusive.

Vom 20.06. bis 03.07.2009 erfahren Sie bei unserer einzigen diesjährigen Veranstaltung zum Thema Information Security Management alles über Konzepte, Praxiserfolge und konkrete Umsetzung.

Stichwort Umsetzung: Erfolgreiche Forensik benötigt komplexe organisatorische und technische Vorgehensweisen. Bei uns lernen Sie diese kennen und können sie aktiv einüben – vom 07. bis 10.07.2009.

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

Nächste KA-IT-Si-Events

Die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) stellt seit ihrer Gründung im Januar 2001 auf fünf bis sechs Abendveranstaltungen pro Jahr aktuelle Themen der IT-Sicherheit in den Fokus. Am 07.05.2009 widmet sich Rüdiger Kügler von WIBU SYSTEMS – einem der Pioniere auf dem Markt für Softwarelizenzmanagement – in seinem Fachvortrag dem Schutz digitaler Güter vor Plagiaten. Im Anschluss werden die Diskussionen beim "Buffet-Networking" wie gewohnt vertieft.

Am 25.06.2009 wird Peter Zimmer von der prego services GmbH einen Erfahrungsbericht zur Zertifizierung nach dem Sicherheitsstandard ISO 27001 vorstellen. Für beide Events bitten wir um rechtzeitige Anmeldung unter www.ka-it-si.de.

Veranstaltungshinweise

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

Mai 2009	
05.-07.05.	10. Datenschutzkongress 2009 (EUROFORUM, Berlin)
07.05.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
18.-20.05.	IFIP SEC 2009 (IFIP, Zypern/CY)
20.-22.05.	2009 ADFSL Conference on Digital Forensics, Security and Law (ADFSL, Burlington/US)
Juni 2009	
02.-05.06.	ACNS '09: International Conference on Applied Cryptography and Network Security (INRIA, Paris/FR)
03.-04.06.	ASIA '09: 4th Annual Symposium on Information Assurance (University at Albany, Albany/US)
08.-09.06.	DuD 2009 (Computas, Berlin)
21.-25.06.	Africacrypt 2009 (IACR, Gammarth/TN)
22.-26.06.	T.I.S.P. Schulung (Secorvo College)
30.06.-03.07.	Information Security Management (Secorvo College)

Fundsache

Die Mustervertragsanlage des Bitkom zur Auftragsdatenverarbeitung liegt nun in einer um eine englische Übersetzungshilfe erweiterten Fassung 2.1 vor. Die auf das Wesentliche beschränkte (und als Word-Formular verfügbare) Vertragsvorlage zur Umsetzung der Anforderungen aus § 11 BDSG an die Verarbeitung personenbezogener Daten im Auftrag liefert eine wertvolle Grundlage für die Erstellung angepasster Vertragsentwürfe – und wird insbesondere mittelständischen Unternehmen ans Herz gelegt.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch

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