secorvo
security consulting

Secorvo Security News

Dezember 2011

Macht verpflichtet

Jede Führungskraft und jedes Staatsoberhaupt sollte es wissen: Mit Macht und Einfluss wachsen nicht nur die Rechte, sondern vor allem die Pflichten.

Die stehen aber oft auf keinem Papier, sondern sind Teil eines „ethischen Codex", wurden durch Kollegen oder Vorgänger vorgelebt oder gehören zur allgemeinen Erwartungshaltung an die jeweilige Position. Das macht es den Betroffenen nicht leicht: Was gestern noch zulässig, unanstößig oder tolerabel war, kann in einer neuen Rolle ein absolutes „No-Go" sein. Ohne eine mentale Umstellung geht das schnell schief – enge, langjährige Freundschaften geraten in den Verdacht der Vorteilsnahme, und die „unbürokratische" Durchsetzung von Entscheidungen riecht schnell nach Amtsmissbrauch. Der souveräne Umgang mit Macht erfordert Selbstdisziplin und vorbildliches Verhalten ebenso wie die Beachtung von Regeln und Kontrollen, und manchmal auch Verzicht.

Das gilt auch für Administratoren. Denn die für den IT-Betrieb Zuständigen sind mit großer Machtfülle ausgestattet: Sie besitzen weit gehende Zugriffsberechtigungen, haben Einblick in detaillierte Log-Protokolle und verfügen über mächtige Analyse-Tools. Mit der Selbstdisziplin ist es allerdings oft nicht weit her: Immer wieder existieren gemeinsame Admin-Passworte, werden aus unsicherer Quelle Programme geladen und ungeprüft installiert oder aus Neugierde Logdaten ausgewertet. Selbst vor dem Lesen vertraulicher Dokumente oder der E-Mails von Kollegen schrecken einige Administratoren nicht zurück. In dieselbe Richtung weist eine Studie der Fa. Balabit vom 15.11.2011: Danach gaben 74 % der anonym Befragten Administratoren zu, ihre Rechte bereits missbraucht zu haben.

Dabei sollten die Passwörter von Admins besonders lang, Logfiles und Daten im Normalbetrieb tabu, die Rechte auf das Erforderliche beschränkt und auf allen Rechnern nur lizenzierte und freigegebene Software installiert sein. Nicht nur Führungskräfte und Staatsoberhäupter, sondern auch „Admins" haben eine Vorbildfunktion.

Inhalt

secorvo
security consulting

Security News

Advent, Advent, der Drucker brennt...

Am 29.11.2011 wurden Forschungsergebnisse publik, nach denen HP-Druckern mittels eines manipulierten Druckauftrags ein Firmware-Update untergeschoben werden kann. Das von den Medien begierig aufgegriffene Detail, dass damit durch Überhitzung der Fixiereinheit möglicherweise ein Druckerbrand ausgelöst werden könnte, erwies sich jedoch als Falschmeldung: Laut HP verfügen die Drucker über einen Überhitzungsschutzschalter, der nicht per Firmware beeinflusst werden kann.

Ebenso als Falschmeldung erwies sich die Nachricht vom 18.11.2011, wonach Hacker eine Pumpe in einem amerikanischen Wasserwerk zerstört hätten: Am 30.11.2011 erklärte ein Techniker, dass er aus seinem Russland-Urlaub versucht hatte, die defekte Pumpe per Remote-Wartung wieder in Gang zu bekommen.

Trotz dieser spektakulären Advents-Enten sollte man sich nicht in falscher Sicherheit wiegen, denn in beiden steckt ein wahrer Kern: Die (Un-)Sicherheit von digitalen Prozessteueranlagen ist bekannt, und spätestens seit Woz' trickreicher Apple-II-Floppy weiß man, dass es ein Wettbewerbsvorteil sein kann, Funktionen aus teurer Hardware in billige Firmware zu verlagern. Wenn das allerdings kritische Funktionalität betrifft, muss sich der Hersteller intensiv um die Firmware-Integrität kümmern.

Und sie ist doch personenbezogen...

Der EuGH hat am 24.11.2011 auch den Versuch einer belgischen Urheberrechtsverwertungsgesellschaft (SABAM) abgewiesen, einen Internet-Provider (Scarlet Extended SA) zur Implementierung eines P2P-Inhaltsfilters zu verpflichten.

Danach schränkt der Zwang, ein Filtersystem über sämtliche Inhalte auf eigene Kosten zu betreiben, die Provider in ihrem Recht auf unternehmerische Freiheit (Art. 16 der Charta der Grundrechte der EU) ein und schafft keinen angemessenen Ausgleich zwischen den betroffenen Grundrechten. Hierbei sei auch Art. 15 der Richtlinie 2000/31/EG (Richtlinie über den elektronischen Geschäftsverkehr) zu beachten, der es untersagt, Diensteanbietern eine allgemeine Überwachungspflicht aufzuerlegen. Zudem würden das Recht der Nutzer auf den Schutz personenbezogener Daten und auf Informationsfreiheit (Art. 8 und 11 der Charta) unzulässig eingeschränkt.

Bemerkenswert ist die uneingeschränkte Einstufung der IP-Adressen als personenbezogene Daten durch den EuGH – ein großer Schritt zur Klärung dieser wichtigen datenschutzrechtlichen Streitfrage.

Content Security Standard

Bereits in den SSN 09/2010 hatten wir über das Mozilla-Konzept einer Content-Security-Policy (CSP) zur Server-gesteuerten Kontrolle aktiver Inhalte in Webseiten berichtet, das seit Version 4 von Firefox unterstützt wird.

Inzwischen wurde auch bei Google Chrome und dem Internet Explorer mit der Integration begonnen. Bei den Konkurrenzbrowsern dürfte wesentlich zur Motivation beigetragen haben, dass der Ansatz inzwischen durch das W3C gesteuert wird: Seit dem 12.12.2011 liegt ein überarbeiteter CSP-Entwurf für einen W3C-Standard vor. Es darf also erwartet werden, dass sich dieser wirksame Ansatz zum Schutz vor Cross-Site Scripting durchsetzen wird.

Datenschutz per Verordnung

Die Europäische Kommission hat am 29.11.2011 einen länger erwarteten Entwurf einer Datenschutzverordnung vorgelegt. Eine EU-Verordnung ist, anders als eine Richtlinie, unmittelbar geltendes Recht – kein unbedeutendes Dokument also.

In großen Teilen entspricht der knapp 80seitige Verordnungsentwurf bereits geltendem deutschem Datenschutzrecht oder greift Rechtsmeinungen der Aufsichtsbehörden auf. Allerdings schließt er auch Regelungslücken und verschärft die eine oder andere Bestimmung. So zählt die Verordnung alle Personen, die mit vernünftigerweise zu erwartenden Mitteln durch einen beliebigen Dritten identifiziert werden können, zu den Betroffenen (Art. 3). Zudem wird der Anwendungsbereich ausdrücklich auf das Veröffentlichen an einen unbestimmten Personenkreis erweitert (Art. 2).

Die Verschärfungen betreffen u. a. die Vorabkontrolle, die zu einer Risiko- und Folgenabschätzung ausgebaut wird (Art. 30). Die bisherigen Prinzipien (Verbot mit Erlaubnisvorbehalt, Erforderlichkeit, Zweckbindung und Transparenz) werden um das Recht auf Löschung und Vergessen ergänzt (Art. 15) – ein Prinzip, dass ebenso wie die neue Forderung nach Datenschutz durch Technikgestaltung und datensparsame Grundeinstellungen (Art. 20) insbesondere auf Social Networks abzielt. Enttäuschend ist der Empfehlungscharakter der Bestimmung zu Datenschutz-Siegeln und Zertifikaten (Art. 36).

Gleichzeitig wird die geteilte Verantwortlichkeit für Datenverarbeitungen anerkannt (Art. 21). Die Pflicht zur Bestellung eines Datenschutzbeauftragten wird auf Unternehmen mit mehr als 250 Beschäftigten oder besonderen Verarbeitungen beschränkt (Art. 32-34). Eingeführt werden auch

verbindliche Unternehmensrichtlinien als Grundlage des Datenexports in Drittstatten (Art. 40).

Die Durchsetzung wird durch ausführliche Vorgaben und erweiterte Befugnisse für die zu schaffende Aufsicht (Art. 43 ff) und Strafvorschriften (Art. 78 f) sowie Haftungsregeln (Art. 77) gestärkt.

Zwar ist zu erwarten, dass der Entwurf noch eine Reihe von Änderungen erfahren wird. Dennoch dürfte er endlich wieder Leben in die festgefahrene deutsche Diskussion um ein modernes Datenschutzrecht bringen.

Weihnachtsgeld

Weihnachtszeit ist Shopping-Zeit: Die Wochen vor Weihnachten sind nicht nur für Einzelhändler, sondern auch für Online-Shops die umsatzstärkste Jahreszeit. Dass wissen auch Black Hats – und drohen vermehrt mit DDoS-Attacken, die sie erst nach Zahlung eines Schutzgelds via Western Union aussetzen oder einstellen.

Am 20.12. erwischte es Conrad Electronic, am 21.12. den Webhoster Mittwald CMS, und am 22.12.2011 war der Werbemittelversand schneider nicht erreichbar. Nach Auskunft des Bundesverbands des deutschen Versandhandels (bvh) ergab eine Umfrage des britischen e-retailing-Verbands imrg, dass bereits 20 % der E-Commerce-Unternehmen von dieser modernen Form der Schutzgelderpressung betroffen sind.

Kein Wunder, dass Analysten technischen Schutzmaßnahmen gegen gezielte DDoS-Angriffe ein erhebliches Marktwachstum prophezeihen – nach über 50% in 2011. Aber auch mit Bordmitteln kann man vielen DDoS-Angriffen etwas entgegensetzen – eine schöne Übersicht solcher Maßnahmen hat Moritz Jäger am 27.02.2011 publiziert.

Bin schon da!

Alle Arten von Smartphones sind grundsätzlich durch Apps gefährdet, die Schadfunktionen enthalten – das ist nichts Neues. Neu ist, dass auch von vorinstallierten Tools eine Bedrohung ausgehen kann. Der Android-Entwickler Trevor Eckart veröffentlichte am 28.11.2011 ein Youtube-Video, in dem er die von US-Providern und Herstellern auf über 141 Mio. Smartphones vorinstallierte App "CarrierIQ" analysierte. Die Ergebnisse seiner Untersuchungen publizierte er inzwischen auch auf seiner Webseite. Die Software, die ursprünglich zur Optimierung von Netzen gedacht war, erlaubt es, Benutzereingaben und weitere Informationen wie die aktuellen GPS-Koordinaten abzugreifen. Allerdings lässt sie sich nicht einfach deaktivieren – und ist zudem in der Lage, sich zu tarnen.

Auch können Android-Apps über vorinstallierte Anwendungen die zugewiesenen Berechtigungen (*permissions*) unterlaufen, wie Forscher der North Carolina State University herausfanden. Sie stellten fest, dass viele vorinstallierte Apps von anderen Apps eingespannt werden können und so restriktiv eingestellte Berechtigungen erweitern (*permission leaks*). Wir empfehlen daher auch vorinstallierte Apps daraufhin zu prüfen, ob man sie wirklich benötigt, und – um die Angriffsmöglichkeiten zumindest etwas einzuschränken – nicht genutzte Apps zu deinstallieren. Auch sollte man die Dienste GPS und WLAN nur dann einschalten, wenn man sie benötigt. Das schafft nicht nur mehr Privatsphäre – sondern erhöht auch die Akku-Laufzeit.

Wir wünschen Ihnen erholsame und schöne Weihnachtsfeiertage – und einen guten Start in ein rundum sicheres Jahr 2012!

Secorvo News

Auf die letzte Minute…

Wer noch ein Plätzchen unter dem Baum zu füllen hat: Wenige Mausklicks genügen, und die „Zentralen Bausteine der Informationssicherheit“ gehören Ihnen – das Grundwissen des T.I.S.P. in 22 Kapiteln, als Nachschlagewerk oder zur Vorbereitung auf eine T.I.S.P.-Zertifizierung (79,95 Euro).

Krypto live

Ab 2012 wird eine Kooperation mit dem Karlsruher Institute of Technology (KIT) und dem am 17.10. 2011 feierlich eröffneten Kompetenzzentrum für angewandte Sicherheits-Technologie (KASTEL) die Karlsruher IT-Sicherheitsinitiative (kurz: KA-IT-Si) bereichern.

So startet die KA-IT-Si gleich am 26.01.2012 mit einem Highlight: Verschlüsselungstechnik gestern und heute „zum Anfassen“ am Institut für Kryptographie und Sicherheit (IKS) des KIT. Die Veranstaltung beginnt um 18 Uhr im Informatik-Gebäude (50.34) des KIT-Campus Süd, Karlsruhe. Wir freuen uns auf Ihre Teilnahme!

Veranstaltungshinweise

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

Januar 2012	
17.-19.01.	OMNICARD 2012 (in TIME berlin, Berlin)
24.-26.01.	Sicherheitsmanagement heute (Secorvo College, Karlsruhe)
26.01.	Krypto zum Anfassen (KA-IT-Si/KIT, Karlsruhe)
Februar 2012	
08.-09.02.	22. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.-22.02.	19. DFN Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2012	
13.-15.03.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
14.-16.03.	Black Hat Europe 2012 (Blackhat, Amsterdam/NL)
21.-22.03.	Verlässliche Web-Anwendungs-Sicherheit (Secorvo College, Karlsruhe)
26.-30.03.	CPSSE (Secorvo College, Karlsruhe)
April 2012	
23.-26.04.	PKI (Secorvo College, Karlsruhe)
24.-25.04.	Datenschutztage 2012 (Forum für Datenschutz, Wiesbaden)

Fundsache

Der Virenschutzanbieter Kaspersky Lab hat einen „Security-Advents-kalender" herausgebracht – mit 24 kernigen Tipps für eine sichere Weihnachtszeit.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp

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