secorvo
security consulting

Secorvo Security News

Januar 2013

Der dritte Faktor

Jüngst erregten Eric Grosse, Googles Vice President für Security Engineering, und sein Kollege Mayank Upadhyay mit einer Veröffentlichung in der Januar/Februar-Ausgabe von IEEE Security & Privacy Aufsehen. In dem achtseitigen Aufsatz Authentication at Scale stellen sie ihre Konzepte einer skalierbaren und Benutzer freundlichen Zwei-Faktor-Authentifikation vor und bezeichnen Googles two-step verification feature (2sv), „adopted by millions", als eines der „largest two-factor authentication deployments in the world".

Deutschen Online-Bankern dürfte diese Einschätzung höchstens ein mitleidiges Lächeln entlocken – besteht das Verfahren doch im Wesentlichen darin, dass 2sv-Nutzern beim erstmaligen Login auf einem neuen oder fremden Device eine sechsstellige Zufallszahl via SMS zugesandt wird, die sie eintippen müssen: mTAN lässt grüßen.

Insgesamt belegt die Publikation den Erfahrungsrückstand des Internet-Giganten: Das Konzept von „2sv Cookies" als Credential und die Überzeugung, wiederholte Authentifikationen durch „Delegation" an ein Device-Credential vermeiden zu können, entstammen dem prätrojanischen Zeitalter.

Zwar gestehen sie zu, das 2sv durch cleveres Phishing und Malware bedroht sein könnte. Ihre Antwort darauf ist jedoch die Bindung des Cookie-Credentials an den SSL-Client – und nicht die Einsicht, dass Vertrauen in ein programmierbares Mehrzweck-Gerät wie ein Smartphone oder ein PC niemals eine gute Idee sein kann. Denn ein starkes Authentifikationsverfahren braucht einen dritten Faktor: das „uncheatable device" – ein Gerät zur Prüfung und Anzeige eines Credentials, das dem Zugriff eines Angreifers wirksam entzogen ist.

Deutsche Banken und Sparkassen haben das längst verstanden und bieten TAN-Generatoren wie chipTAN oder PhotoTAN, um Überweisungen zu authentisieren. Vielleicht werden diesmal aus den Gejagten die Jäger: Was liegt näher, als solche TAN-Generatoren auch für andere wichtige Authentifikationen zu verwenden?

Inhalt

secorvo
security consulting

Security News

Aus dem Giftschrank

Pass-the-Hash (PtH) und verwandte Attacken sind eine Bedrohung von Windows-Systemen, die seit vielen Jahren bekannt und schwerwiegend, aber nicht prinzipiell auszuschließen sind: Ein Angreifer, der Systemrechte auf einem Windows-System erlangt hat – oder sich gar auf einer der unter Eingeweihten kursierenden Methoden eine permanente Hintertür einrichten konnte – kann mit Tools wie WCE oder mimikatz die Credentials der an diesem System momentan oder kürzlich angemeldeten Benutzer aus dem Hauptspeicher auslesen. Dies betrifft Kerberos-Tickets und NTLM-Hashes, mit denen sich der Angreifer auch ohne Passwort im Netzwerk anmelden kann, LM-Hashes (selbst unter Windows 7), die per Online-Service zu einem Passwort zurück gerechnet werden können, und oft sogar Klartext-Passwörter. Am 11.12.2012 veröffentlichte Microsoft nun ein Whitepaper mit Ratschlägen, wie man derartigen Attacken begegnen kann. Die darin propagierten Ansätze werden von einigen Fachleuten als unzureichend oder praxisuntauglich kritisiert. Einig ist man sich allerdings – auch mit früheren Artikeln – darin, was *nicht* hilft: beispielsweise Smarcard-Logon oder der Verzicht auf NTLM zugunsten von Kerberos.

Alle Empfehlungen laufen letztlich darauf hinaus, es gar nicht erst zu einer Infektion kommen zu lassen: Erstens sollte man unbedingt verhindern, dass Angreifer unter Windows Systemzugriff auf den Hauptspeicher erlangen können (durch eine Vielzahl von ineinander greifenden Maßnahmen von der Festplattenverschlüsselung über Software-Restriction, strikter Kontrolle lokaler Administrationsrechte bis zur Deaktivierung von Schnittstellen). Und zweitens sollte man sich nicht mit hohen Berechtigungen an Maschinen anmelden, bei denen nicht hinreichend sicher ist, dass „Erstens“ erfolgreich war, um einem Angreifer die Credentials nicht auf dem Silbertablett zu servieren.

Gegengift

Die Isolierung des Browsers auf dem eigenen System ist ein probates Mittel zur Eindämmung unerwünschter Infektionsfolgen. Eine nahe liegende Möglichkeit ist das Browsen in virtuellen Maschinen – mit gängigen Virtualisierungslösungen ist das Ergebnis jedoch oft schwergewichtig und behäbig.

Eine leichfüßige Alternative sind Sandbox-Lösungen, mit denen die „Nebenwirkungen“ eines infizierten Objekts im Browser oder Dokumentenviewer eingeschränkt werden können. Beispielhaft sei hier das am 16.12.2012 in Version 3.76 publizierte Tool Sandboxie empfohlen, bei dem alle Schreibzugriffe innerhalb einer geschlossenen Umgebung erfolgen. Wird eine Sandboxie-Session beendet, werden alle Downloads, Änderungen an Dateien usw. zuverlässig verworfen. Das Konzept stellt eine Form des im Editorial der SSN 9/2012 diskutierten Einweg-Paradigmas dar. Im Sinne des *Defense-in-Depth* ist eine solche Sandbox-Lösung ein einfaches, aber wirksames Gegengift gegen unerwünschte Nebenwirkungen.

Umgang mit Giftstoffen

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat am 08.01.2013 eine Broschüre mit Tipps und Informationen zum datenschutzbewussten Umgang mit Facebook herausgegeben. Darin werden anhand von Screenshots die wichtigsten Einstellungen erläutert, die man zum Selbstschutz vornehmen sollte: Verwendung von Pseudonymen (entgegen den unwirksamen Nutzungsbedingungen), Verhinderung von Tracking, Unterbindung der Profilsuche über Google und der Verwendung personenbezogener Daten für Werbeanzeigen. Es wird vor der Facebook-Chronik und der Freigabe eigener Adressbücher für die Freunde-finden-Funktion gewarnt und deutlich auf die Erforderlichkeit einer Einwilligung für die Veröffentlichung von Daten Dritter hingewiesen.

Die Tipps und Hinweise sind leicht verständlich und umfassend. Dabei wird deutlich, wie weit Facebook von „Datenschutz by default“ entfernt ist. Der pragmatische Ansatz, Datenschutz durch Information der Nutzer zu fördern, solange das Durchsetzen der Datenschutzanforderungen bei einem internationalen Anbieter stockt, ist zu begrüßen.

Digitale Giftanalyse

Ist Gefahr im Verzug, muss man schnell handeln. Daher kommt es bei forensischer Incident Response darauf an, mögliche Beweisdaten zügig zu sichern. In der Windows-Systemdatei NTUSER.DAT werden Tätigkeiten des jeweiligen Benutzerkontexts nachvollziehbar gespeichert – die Datei lässt sich im laufenden Systembetrieb und bei angemeldetem Benutzer jedoch weder auslesen noch kopieren, da Windows den Zugriff auf offene Dateien sperrt.

Dieses Zugriffsproblem löst die am 03.11.2012 erschienene Version 0.72 von ntfscopy komfortabel, indem des den Zugriff an der Windows-internen Zugriffskontrolle vorbei ermöglicht. Dabei kann der Slack-Space mitkopiert werden, um bereits gelöschte Einträge zu durchsuchen. Auch die zugehörigen NTFS-Metadaten und NTFS-Dateiattribute, die in der Regel nur sehr schwierig manipulierbar sind, sowie direkte Zugriffe auf einzelne Alternate Data

Streams einer Datei, in denen sich z. B. Malware verstecken kann, können abgespeichert werden.

Daraus extrahiert der Computer Account Forensic Artifact Extractor (cafae) aussagefähige Daten und Zeitstempel u. a. für Benutzerkontenaktivitäten (UserAssist-History, RecentDocs, OpenSavePidlMRU und MountPoints2), z. B. für USB-Geräte. Sehr hilfreich ist, dass die Zeitangaben sowohl im SleuthKit-Bodyformat als auch im log2timeline-Format erzeugbar und so für eine übergreifende Zeitlinienanalyse nutzbar sind.

Die Kehrseite der Medaille: Sicherheitsmanager und Revisoren werden sich zukünftig fragen müssen, wie integer das geprüfte Zugriffsberechtigungskonzept in Windows-NTFS-Dateisystemen ist, wenn solche Zugriffsmöglichkeiten (ohne Auditeintrag im Security-Eventlog) bestehen.

Heimliches Gift

Die Fraktionen von CDU/CSU und FDP überraschten am 10.01.2013 mit einer Neufassung des seit Ende 2010 vorliegenden Gesetzentwurfs zum Beschäftigtendatenschutz. Gegenüber dem bereits kontrovers diskutierten ersten Entwurf enthält die Neufassung einige gewichtige Änderungen: Als § 32m BDSG soll ein Absatz zur Beschäftigtendatenübermittlung im Konzern eingefügt werden, begleitet von Änderungen mit Relevanz für die Auftragsdatenverarbeitung im Ganzen. Der ohnehin schon unübersichtliche § 28 BDSG wird um Sondertatbestände für Beschäftigtendaten erweitert. Die Überwachungsbefugnisse der Arbeitgeber sind über den ersten Entwurf hinaus erweitert worden, etwa im Bereich der Call-Center oder der Videoüberwachung. Weitere Regelungen wurden durch unbestimmte Rechtsbegriffe oder Streichungen verwässert.

Die neu aufgenommenen Regelungen zur Beschäftigtendatenübermittlung im Konzern und zur internationalen Auftragsdatenverarbeitung reagieren auf einen tatsächlichen Bedarf. Sie kodifizieren aber lediglich bislang praktizierte Lösungsansätze. Neue interessensgerechte und vereinfachte Lösungen bringen sie nicht, etwa zur Auftragsdatenverarbeitung in unsicheren Drittstaaten.

Die plötzliche Eile ist angesichts der wenigen echten Innovationen und der vielen Mängel des Gesetzes nicht ratsam: Der Datenschutz braucht durchdachte Lösungen statt gesetzgeberischer Detailkorrektur von Rechtsprechung und -praxis. Das hat nun wohl auch die Bundesregierung eingesehen: Der Entwurf sollte zunächst schon am 16.01.2013 im Innenausschuss verhandelt werden, wurde jedoch kurzfristig – evtl. wegen der sich schnell verbreitenden Proteste aus Datenschutzkreisen – wieder von der Tagesordnung genommen. Am 30.01.2013 sollte er wieder in den Innenausschuss – und wurde am 29.01.2013 erneut von der Tagesordnung gestrichen.

Secorvo News

Winterlektüre

Frühabendliche Dunkelheit und Minustemperaturen laden ein zur gemütlichen Lektüre im Lesesessel oder vor dem Kamin. Sollten Ihnen dabei die Bücher ausgehen, so helfen wir gerne: Neben unserem 520seitigen T.I.S.P.-Buch „Zentrale Bausteine der Informationssicherheit“ können wir Ihnen – abhängig von Ihren fachlichen Präferenzen – Michael Knopps Aufsatz über Google und den Datenschutz (DANA 12/2012), Dr. Safuat Hamdys Beitrag über den OWASP Application Security Verification Standard (DuD 11/2012) und Hans-Joachim Knobloch Vorstellung des zukünftigen SHA-3-Hash-Standards *Keccak* (KES 1/2013) ans Herz legen.

Zertifikate

Sollte sich unter Ihren guten Vorsätzen für das neue Jahr auch die Zertifizierung Ihrer Kenntnisse und Erfahrungen in der Informationssicherheit finden, können wir auch hier helfen: das nächste T.I.S.P.-Seminar findet statt vom **15.–19.04.2013** mit anschließender Prüfung am 20.04.2013. Die nächste CPSSE-Zertifizierung in sicherer Softwareentwicklung bieten wir bereits vom **11.–14.03.2013** an. Erstmalig zählt in diesem Jahr auch ein Seminar zu „Security by Design“ zu unserem Seminarangebot: Security Engineering vom **18.–21.03.2013**. Wir freuen uns darauf, Sie zu einer dieser Veranstaltungen bei uns begrüßen zu dürfen!

Alle Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter
http://www.secorvo.de/college

Ausgebucht

Gerne hätten wir an dieser Stelle noch einmal für das KA-IT-Si-Event am 31.01.2013 im Karlsruher Zentrum für Kunst und Medientechnologie (ZKM) geworben, an dem die dreitätige Ausstellung des Kompetenzzentrums für Angewandte Sicherheits-Technologie (KASTEL) am KIT, „Kryptologikum – Kryptographie begreifen“ eröffnet wird. Mit über 200 Teilnehmern ist die Veranstaltung jedoch seit einer Woche komplett ausgebucht – und wir müssen auf die Ausstellung selbst vertrösten, die vom **01.–03.02.2012** im ZKM kostenlos besucht werden kann. Dafür bitten wir Sie, schon einmal den nächsten Termin vorzumerken: Das zweite diesjährige Event der KA-IT-Si findet statt am **14.03.2013** – Details folgen.

Veranstaltungshinweise

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

Februar 2013	
01.-03.02.	Kryptologikum (KIT/KASTEL, ZKM Karlsruhe)
06.-07.02.	23. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
15.-17.02.	ShmooCon 2013 (The Shmoo Group, Washington/US)
19.-20.02.	20. DFN-Workshop „Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
März 2013	
05.-09.03.	CeBIT (Deutsche Messe, Hannover)
11.-14.03.	CPSSE-Schulung (Secorvo College, Karlsruhe)
12.-15.03.	Black Hat Europe 2013 (Blackhat, Amsterdam/NL)
18.-21.03.	Security Engineering (Secorvo College, Karlsruhe)
April 2013	
09.-11.04.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
15.-19.04.	T.I.S.P.-Schulung (Secorvo College, Karlsruhe)
17.-18.04.	a-i3/BSI Symposium 2013 (a-i3/BSI, Bochum)
23.-26.04.	PKI (Secorvo College, Karlsruhe)

Fundsache

In diesem Jahr macht Deloitte den Anfang: Die 2013 TMT Global Security Study gibt einen Einblick in die Einschätzungen, Schwerpunkte und Investitionen der 120 größten Unternehmen der Telekommunikations-, Medien- und Technologiebranche. Eine der zentralen Herausforderungen: "*Lack of sufficient awareness with employees*" (70 %).

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Hans-Joachim Knobloch, Michael Knopp, 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