secorvo
security consulting

Secorvo Security News

September 2017

Sie haben die Wahl...

Am 07.09.2017 sorgte der Chaos Computer Club (CCC) kurz vor der Bundestagswahl für Aufregung: Er hatte zahlreiche Schwachstellen in der Software ‚PC-Wahl' identifiziert. Diese Software dient zwar nur zur Ermittlung des vorläufigen Endergebnisses, dennoch könnte dessen Manipulation zu einem Chaos und einer Verunsicherung der Bevölkerung führen. Ein derartiger Vorfall dürfte auch das Vertrauen in den Wahlvorgang nachhaltig erschüttern.

Das Thema Wahlcomputer und Online-Wahlen hielten viele nach dem Urteil des Bundesverfassungsgerichts (BVerfG) im Jahr 2009 für abgeschlossen. Dennoch brachte BSI Präsident Arne Schönbohm in einem Interview vom 11.09.2017 das Thema Online-Wahlen für die nächste Legislaturperiode ins Gespräch. Mit seiner Kritik an der Briefwahl schlägt Prof. Dr. Müller-Quade – Gewinner des deutschen IT-Sicherheitspreises für das Bingo-Voting-Verfahren – in eine ähnliche Kerbe.

Alle denkbaren kryptografischen Wahlverfahren basieren jedoch auf der Grundannahme, dass die Sicherheit des unterliegenden Wahl-Clients gewährleistet sein muss. Das ist gerade bei Online-Wahlen eine wohl kaum umsetzbare Voraussetzung, zumal viele Wahlberechtigte erreicht werden müssen. Dies ist ein bekanntes Problem der IT-Sicherheit: Immer neue Angriffe auf das Online-Banking zeigen, dass es den Banken trotz Jahrzehnten Erfahrung bisher nicht gelungen ist, eine für den Anwender benutzbare und von der Sicherheit des Client unabhängige Online-Banking-Anwendung zu entwickeln. Das lässt sich auf Online-Wahlen übertragen. Komplexe technische Lösungen behindern zudem die vom BVerfG geforderte Überprüfbarkeit der Wahl durch den Bürger – ohne besondere Sachkenntnis – und lösen daher das grundlegende Problem nicht.

Inhalt

secorvo
security consulting

Security News

Vertrauen entzogen

In der März-Ausgabe (SSN 3/2017) berichteten wir von dem Zertifikatsdesaster von Symantec. Bereits damals waren die Google-Chrome-Entwickler entschlossen, den von Symantec ausgestellten SSL/TLS-Zertifikaten das Vertrauen zu entziehen. Nach längeren Diskussionen und Verhandlungen verkündete Google nun am 11.09.2017 in seinem Security Blog den genauen Zeitplan für diesen in der PKI-Geschichte einmaligen Vorgang. Ausgelöst von Googles Vorstoß hatte Symantec bereits am 02.08.2017 den Verkauf seiner Trustcenter-Sparte an den Mitbewerber DigiCert bekanntgegeben.

Spätestens zum 01.12.2017 sollen Zertifikate für Kunden der (Ex-)Symantec-Marken über DigiCerts Trustcenter-Infrastruktur erstellt werden. Sollten nach diesem Stichtag noch Zertifikate von Symantecs jetziger Infrastruktur ausgestellt werden, wird Chrome diesen nicht mehr vertrauen. Vorhandene Zertifikate, die von Symantecs Trustcenter-Marken (u. a. VeriSign, Thawte und GeoTrust) vor dem 01.06.2016 ausgestellt wurden, verlieren mit dem Erscheinen der Chrome-Version 66 ihre Gültigkeit (geplant für den 15.03.2018). Symantec-Zertifikaten, die zwischen dem 01.06.2016 und dem 01.12.2017 erstellt wurden, soll spätestens mit Erscheinen der Chrome-Version 70 das Vertrauen entzogen werden (geplant für den 13.09.2018).

Mozilla hat bereits angekündigt, sich diesem Zeitplan (bis auf wenige Tage Abweichung aufgrund der Release-Zyklen des Firefox-Browsers) anzuschließen. Betroffene Serverbetreiber sollten sich daher frühzeitig um neue Zertifikate von Symantec/DigiCert oder anderen Anbietern kümmern.

BlueBorne

Insgesamt acht kritische Lücken in den Bluetooth-Stacks entdeckten Sicherheitsforscher von Armis Labs und publizierten diese am 12.09.2017 in ihrem Blog. Vier dieser Schwachstellen erlauben einem Angreifer, Schadcode auf allen gängigen Android-, Linux-, Windows- und iOS-Geräten (mit iOS Versionen bis einschließlich 9.3.5) auszuführen: Zwei ermöglichen das Extrahieren sensibler Informationen unter Linux und Android, die beiden anderen Man-in-the-middle-Angriffe unter Windows und Android.

Das Fatale an den gefundenen Schwachstellen ist die Möglichkeit, ein Gerät anzugreifen, ohne es zuvor mit dem Gerät des Angreifers zu koppeln. Es genügt, eine eingeschaltete Bluetooth-Schnittstelle beim Opfer. Unsichtbare Bluetooth-Geräte sind ebenfalls nicht wirksam geschützt. Zwar konnten Microsoft, Google und die Linux-Foundation im September passende Patches für alle betroffenen Geräte bereitstellen; ob diese jedoch von den Herstellern zügig verbreitet werden, ist vor allem bei Android unsicher. Die Bluetooth-Schnittstelle sollte daher deaktiviert werden, bis eine entsprechende Aktualisierung erfolgt ist.

Malware mit Brief und Siegel

Am 18.09.2017 wurde bekannt, dass das beliebte Festplatten-Bereinigungstool CCleaner etwa vier Wochen lang mitsamt einem Trojaner ausgeliefert wurde. Besonders pikant daran ist zum einen, dass kurz zuvor CCleaner-Hersteller Piriform vom Antiviren-Unternehmen Avast übernommen worden war. Zum anderen trugen die befallenen Softwarepakete gültige Code-Signaturen von Piriform. Dennoch braucht der Hersteller wohl keine Welle an Schadenersatz-Klagen aufgrund einer irgendwie gearteten Produkthaftung zu befürchten, was auch die am 19.09.2017 abgewiesene Klage FTC gegen D-Link unterstreicht.

Entdeckt wurde die Schadsoftware unabhängig voneinander in Kunden-Installationen zweier Unternehmen, die aufwändige neuere Ansätze beim Malwareschutz verfolgen. Der klassische, signaturbasierte Virenschutz dagegen gelangte wieder einmal an seine Grenzen: Selbst nach dem Bekanntwerden vergingen noch ca. drei Tage, bevor ein Großteil der unter VirusTotal versammelten Virenscanner den befallenen Installer nicht mehr als „Clean“ meldete. Die Aufarbeitung des Vorfalls folgt eher dem herkömmlichen Muster: Nach ersten Beschwichtigungen, eine Sekundärinfektion wäre unwahrscheinlich, ergab die forensische Analyse des beschlagnahmten C&C-Servers doch knapp zwei Dutzend auf eben diese Weise angegriffene Unternehmen. Inzwischen ist von APT, bekannten Angriffsmustern und asiatischen Netzwerken die Rede – gäbe es die sprichwörtlichen ‚Chinesischen Hacker' nicht, man müsste sie als Synonym für „höhere Gewalt“ erfinden.

Angesichts der Zunahme von „Supply Chain Attacks“ ist jedoch der Blick nach vorn wichtiger als die Suche nach Entschuldigungen. Ein erster Schritt könnte sein, dass Softwarehersteller im Freigabeprozess ihre Softwarepakete zunächst eine Weile mit neueren, bspw. verhaltensbasierten Anti-Malware-Methoden prüfen, ehe sie per Code-Signatur die – wenn schon nicht justiziable, so doch moralische – Verantwortung für ihren so versiegelten Code übernehmen.

Neues vom Privacy Shield

Seit dem 01.08.2016 ist das Europäisch-US-amerikanische Privacy Shield eine Alternative zu den übri-

gen Wegen, die ein gleichwertiges Schutzniveau bei der Verarbeitung personenbezogener Daten sicherstellen sollen. Teil des Abkommens ist eine Beschwerdemöglichkeit, zu deren Unterstützung mehrere deutsche Datenschutzaufsichtsbehörden nun ein Beschwerdeformular publiziert haben.

Das Formular erfragt die erforderlichen Informationen zur Überprüfung der Datenübermittlung ab. Die Beschwerde kann dann von einer unabhängigen Stelle bearbeitet werden. Führt dies nicht zu Abhilfe bleibt dem Betroffenen die Beschwerde bei den eigenen lokalen Datenschutz-Aufsichtsbehörden.

Das Formular ist eine Erleichterung zur Wahrung der Betroffenenrechte. Ob das Instrument jedoch tatsächlich zu einem verbesserten Schutz der personenbezogenen Daten führt, ist zweifelhaft: Nur wenige Betroffene werden überhaupt von der Möglichkeit zur Nachforschung wissen, geschweige denn den dafür erforderlichen Aufwand treiben.

Weitere IT-Sicherheitspflichten

Am 30.06.2017 ist weitgehend unbemerkt das Umsetzungsgesetz zur Richtlinie EU 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (kurz: NIS-Richtlinie) in Kraft getreten. Die Neuregelungen für Anbieter digitaler Dienste gelten ab dem 10.05. 2018. Das Gesetz nimmt auch zahlreiche Änderungen an den durch das IT-Sicherheitsgesetz eingeführten Bestimmungen vor.

Kern ist die Erweiterung des BSI-Gesetzes um einen § 8c, der die Anbieter zum Ergreifen verhältnismäßiger technischer und organisatorischer Maßnahmen verpflichtet, eine Meldepflicht für erhebliche Vorfälle einführt und das BSI zur Prüfung sowie zum Erlass von Anordnungen ermächtigt. Mit ‚digitalen Diensten' sind Dienste der Informationsgesellschaft gemeint, einschließlich Online-Marktplätzen, Suchdiensten und Cloud-Diensten.

Die sonstigen Befugnisse des BSI werden um Regelungen zu Mobilen Incident Response Teams (MIRTs) ergänzt, die andere Stellen nach Sicherheitsereignissen bei der Wiederherstellung ihrer Systeme unterstützen sollen. Auch in Bezug auf die digitalen Dienste wird eine Mitwirkungspflicht von Anwendungsherstellern eingeführt. Die Erweiterungen bezüglich der Betreiber Kritischer Infrastrukturen beziehen sich hauptsächlich auf die Behandlung grenzüberschreitender Belange.

Mit dem Umsetzungsgesetz wird ab Mai 2018 ein weiterer Anbieterkreis gesetzlich zur IT-Sicherheit verpflichtet. Nach den bisherigen Erfahrungen mit dem IT-Sicherheitsgesetz wird sich die Begeisterung bei den betroffenen Unternehmen wohl in Grenzen halten.

Secorvo News

Secorvo Seminare

Noch vier Gelegenheiten zur Weiterqualifikation bieten wir Ihnen in diesem Herbst:

- das T.P.S.S.E.-Seminar zur sicheren Software-Entwicklung (**16.–19.10.2017**),
- unser PKI-Seminar (**06.–09.11.2017**),
- IT-Sicherheit heute (**21.–23.11.2017**) und
- das T.I.S.P.-Seminar (**27.11.–01.12.2017**)

Alle Seminare sind bereits gut gebucht – wir empfehlen daher eine schnelle Anmeldung und freuen uns auf Ihre Teilnahme. Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

CyberWehr-Gipfel in Karlsruhe

Um den wachsenden Schäden durch Cyberangriffe zu begegnen, plant Innenminister Strobl den Aufbau einer CyberWehr Baden-Württemberg. Auf Einladung des Wirtschafsrats wird er das Konzept am **11.10.2017** in einer Keynote auf dem in Zusammenarbeit mit der KA-IT-Si veranstalteten CyberWehr-Gipfel im ZKM | Karlsruhe vorstellen und sich anschließend mit weiteren Experten der Diskussion stellen (Teilnahme frei; zur Anmeldung).

Watching. You.

Als einer der Partner der IT-Sicherheitsregion Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem ZAK | Zentrum für Angewandte Kulturwissenschaft und Studium Generale am **19.10.2017** zum Filmevent in die Karlsruher Schauburg. Bei der Eröffnungsveranstaltung der Traumfabrik #14/2017-18 „BIG BROTHER – Surveillance Cinema" wird der Oscar-prämierte Film „Citizenfour" von Laura Poitras gezeigt, der einen persönlichen Blick auf das Leben von Edward Snowden gibt. Wolfgang Petroll wird eine Einführung in den Film geben; im Anschluss folgt eine Diskussion mit Dr. Oliver Raabe (Zentrum für Angewandte Rechtswissenschaft), Prof. Dr. Caroline Robertson-von Trotha (ZAK), Dr. Dirk Achenbach (Kompetenzzentrum IT-Sicherheit) und Jan Linders (Badisches Staatstheater Karlsruhe).

Danach bieten wir Ihnen wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

Oktober 2017	
10.-12.10.	it-sa 2017 (Nürnberg Messe, Nürnberg)
11.10.	Wehrhafte IT-Sicherheit: Cyberwehr-Gipfel in Karlsruhe (Wirtschaftsrat Deutschland/ Wirtschaftsjunioren Karlsruhe/KA-IT-Si, Karlsruhe)
16.-19.10.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
18.10.	Swiss Cyber Storm 2017 (Swiss Cyber Storm Association, Luzern/CH)
19.10.	Watching. You. (Partner der IT-Sicherheitsregion Karlsruhe/ZAK, Karlsruhe)
24.-26.10.	heise devSec 2017 (dpunkt.verlag, Heidelberg)
November 2017	
06.-09.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
14.-15.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-17.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
15.-17.11.	41. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit, Köln)
21.-23.11.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.11.-01.12.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick (Editorial), Fabian Ebner, 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