Zwischenbericht DigiNotar Certificate Authority Hack und Relevanz für Österreich

Autoren:

L. Aaron Kaplan (kaplan@cert.at)
Otmar Lendl (lendl@cert.at)

Datum: 8.9.2011
Version: 1.0

Executive Summary

Was ist passiert?

Anfang September wurde bekannt, dass ein Angreifer in die niederländische Certification Authority (CA) „DigiNotar“ eingebrochen hatte und sich unbefugt Zertifikate für diverse Domains (u.A. google.com) ausgestellt hatte. Diese wurden für Abhörangriffe auf Iranische Bürger benutzt.

Die betroffenen CAs[1] wurden inzwischen von einigen Browser- und Betriebssystemherstellern aus deren Systemen gestrichen, dadurch werden auch legitime Zertifikate von DigiNotar nicht mehr als gültig anerkannt.

Da Zertifikate von DigiNotar in den Niederlanden für die staatlichen Public-Key-Infrastructure benutzt werden, hat dieser Angriff ernste Folgen für die dortige IT-Infrastruktur[2].

Empfehlungen

- Prüfen Sie, ob in Ihrem Unternehmen Zertifikate von DigiNotar im Einsatz sind - wenn ja tauschen Sie diese aus.
- Stellen Sie ein Update sämtlicher Rootzertifikate bzw. Widerrufslisten aller IT-Systeme sicher. Überprüfen Sie auch in diesem Rahmen, ob Widerrufslisten oder OCSP aktiv verwendet werden
- Erstellen Sie ein zentrales Inventar wo in Ihrem Unternehmen welche Zertifikate im Einsatz sind und von welcher CA diese stammen.
- Planen Sie proaktiv, was Sie im Falle einer Kompromittierung einer von diesen CAs tun würden.

[1] DigiNotar betreibt nicht nur eine CA, siehe Anhang 1.
[2] http://online.wsj.com/article/SB10001424053111903648204576554630259605332.html
http://www.itworld.com/government/200951/dutch-government-struggles-deal-diginotar-hack

Hintergrund

Dieses Dokument basiert auf öffentlichen Informationen von GovCERT.nl, diversen Medienberichten und dem Vorabbericht von Fox-IT[3].

Anfang September wurde bekannt[4], dass die niederländische Certification Authority (CA) „DigiNotar kompromittiert wurde. Es ist davon auszugehen[5], dass es sich um den selben Angreifer wie beim Comodo Hack[6] handelt. Dieser hat eine unbekannte Anzahl von Zertifikaten erstellt. Bei einem Teil der falschen Zertifikate ist bekannt, für welche Namen sie ausgestellt wurden.

Dank der Logfiles vom OCSP Dienst (Online Certificate Status Protokoll), konnte eruiert werden, von wo die meisten Anfragen bzgl. der gefälschten Zertifikate kamen: aus dem Iran. Man kann davon ausgehen, dass diese Zertifikate (wahrscheinlich in Verbindung mit DNS-Poisoning oder Traffic Interception) für eine Man-in-the-middle (MITM) Attacke genutzt wurden. Da www.facebook.com und www.google.com betroffen waren, könnte so massiv in die private Kommunikation der iranischen Bevölkerung eingebrochen worden sein.

Per OCSP werden die falschen Zertifikate jetzt schon enttarnt, auch Firefox, Microsoft, Google und andere haben Updates für ihre Software herausgegeben, die die betroffenen CAs als ungültig markierten. Da der Angreifer weitere, uns noch unbekannte Zertifikate erstellen konnte, muß man derzeit mit SSL MITM Attacken rechnen, die auf noch ungepatchten Systemen nicht auffallen würden.

Die Liste der bekannten, gefälschten Zertifikate ist öffentlich bekannt, siehe Anhang 1.

Die aktuellste Entwicklung zum Zeitpunkt dieses Berichtes war, dass der Comodo Hacker in pastebin[7] Erklärungen abgibt. Darin wird behauptet, dass er auch GlobalSign gehackt hat. GlobalSign hat darauf hin die Ausstellung von Zertifikaten gestoppt und untersucht die Aussage[8].

DigiNotar betreibt sowohl eine sub-CA für die offizielle PKI der niederländischen Regierung als auch eine normale kommerzielle Root-CA für die Öffentlichkeit. Die Regierungs sub-CA wurde zwar ebenfalls kompromittiert, aber es wurden dort – laut unserem Wissen – keine falschen Zertifikate ausgestellt.

DigiNotar wurde kritisiert, da sie von dem Hack seit Juli wussten, aber die betroffenen Stellen und die Öffentlichkeit nicht informierten. Mittlerweile hat der niederländische Staat die Kontrolle über die DigiNotar CA übernommen.

Auswirkungen auf Österreich

Ein Angriff wie jener im Iran hätte potentiell auch österreichische Systeme treffen können. Mildernd wirkt hier, dass für einen MITM – Attack auch eine Umleitung der Kommunikation nötig ist. Das ist im kleinen Maße in lokalen Netzen relativ einfach zu erreichen, für einen breiten Angriff sind dazu aber Manipulationen im DNS oder auf IP-Routing-Ebene nötig. Dafür gibt es in Österreich keine Hinweise.

[3] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html
[4] https://blog.torproject.org/blog/diginotar-debacle-and-what-you-should-do-about-it
[5] http://www.f-secure.com/weblog/archives/00002231.html
[6] http://news.cnet.com/8301-31921_3-20046340-281.html
[7] http://pastebin.com/u/ComodoHacker
[8] http://www.globalsign.com/company/press/090611-security-response.html

Im Gegensatz zu den Niederlanden, wo DigiNotar-Zertifikate Teil der staatlichen PKI sind, erwarten wir nicht, dass diese in Österreich in relevanter Zahl eingesetzt sind. Der Verlust der CA sollte Österreich daher nur marginal treffen.

Der Hacker prahlt damit, dass er auch weitere CAs unterwandert hat. Das könnte für Österreich relevanter werden, insbesondere falls eine CA betroffen ist, deren Marktanteil in Österreich (im Gegensatz zu DigiNotar) nicht vernachlässigbar ist.

Die Hersteller von Browsern und Betriebssystemen haben begonnen, die betroffenen CA-Keys als ungültig zu markieren. Damit werden auch korrekte Zertifikate als ungültig behandelt. Das mag bei Webservern noch relativ harmlos sein (der User kann die Warnung des Browsers ignorieren), kann aber potentiell bei im Hintergrund ablaufenden Kommunikationsprozessen (B2B, Transaktionen zwischen Behörden, Chipkarten, …) fatal sein.

Lessons learned

Die Kompromittierung eines Enduser-Zertifikates ist ein normaler Prozess in PKI-Systemen, der zwar mühsam ist, aber funktioniert, solange OCSP oder Zertifikate Revocation Lists wirklich verwendet werden. Hier ist plötzlich eine CA weggebrochen, was ein deutlich komplexeres Problem erzeugt.

Eine Abhängigkeit von der Integrität einer externen CAs muss bei der IT-Planung und die Risikoanalyse von Firmen berücksichtigt werden. Sie sollte im Design nur bewusst eingegangen werden. Alternativen könnten Selfsigned+Fingerprints oder eine eigene CA sein.

Die Auswirkungen einer kompromittierten CA sind zu untersuchen und entsprechende Prozesse für den Notfall sollten entwickelt und geprobt werden. Es mag auch Sinn machen, für den Notfall Ersatzzertifikate bereitzuhalten, da die Beschaffung neuer Zertifikate Zeit dauert. Jede Applikation sollte im Notfall auf eine andere CA-Hierarchie umschalten können.

Die Integrität von CAs ist eminent wichtig. Dass ein Audit eines bekannten Hauses[9] keine Probleme gefunden hat, obwohl massive systematische Sicherheitsprobleme vorlagen[10], wirft Fragen über die Zulassung und Kontrolle von CAs auf. Es mag nötig sein, hier nicht nur auf die von den CAs selber bestellten und bezahlten Audits zu vertrauen, sondern deutlich strenger vorzugehen. Wie sich in anderen Bereichen (siehe etwa die Bankenkrise/Ratingagenturen) gezeigt hat, ist es grundsätzlich problematisch, wenn ein Auditor im Auftrag des zu Testenden agiert und letzterer ein positives Ergebnis für seine Geschäft benötigt.

Dieser Einbruch bei der CA DigiNotar ist leider kein Einzelfall mehr. Das PKI-System rund um X.509, so wie es aktuell in Browsern und Betriebssystemen implementiert ist, hat ernste Skalierungsprobleme. Bei einer Zahl von Root-CAs im hohen zweistelligen Bereich ist die Gefahr hoch, dass **eine** davon nicht korrekt arbeitet. Es ist daher zu überlegen, ob man in sensitiven Umgebungen die Zahl der installierten CAs deutlich verringern sollte.

Wie erwähnt wurden in diversen Systemen schon per Update die DigiNotar CA als ungültig markiert. Offen sind vor allem noch Browser von mobilen Geräten und Systeme, die keine automatischen

[9] http://www.diginotar.nl/Portals/7/A-2008-3175-DigiNotar-Mgt%20Assertion%20en%20PwC%20auditors%20report-def.pdf
[10] http://www.heise.de/security/meldung/DigiNotar-Hack-Kritische-Infrastruktur-war-unzureichend-geschuetzt-1337378.html

Updates vom Hersteller erhalten. Insbesondere im Bereich der Absicherung von Transaktionen zwischen Computern (Machine to Machine, M2M) ist hier eine manuelle Kontrolle notwendig.

CERT.at empfiehlt Unternehmen, ein Inventar der im eigenen Haus verwendeten Zertifikate (Webserver, M2M, Client-Zertifikate, Code-Signing, VPN Keys, …) zu erstellen. Falls dabei von DigiNotar signierte gefunden werden, sind diese zu ersetzten. Der Einbruch bei Globalsign ist noch nicht bestätigt, wir empfehlen deren Kunden, die Entwicklung genau zu verfolgen.

Allgemeines

Es hat sich hier wieder gezeigt, wie wichtig eine gute IT-Sicherheit für ein Unternehmen ist. Aus heutiger Sicht hat die Firma DigiNotar mit dem Verlust ihrer Vertrauensposition ihre Geschäftsgrundlage zerstört. Konkret wurden hier folgende Fehler gemacht:

- Eine mangelhafte Passwort-Policy im Unternehmen. Bei DigiNotar waren die Passwörter mittels Wörterbuch-Attacken erratbar.
- DigiNotar hat die Kompromittierung lange nicht erkannt. Es gab zwar ein IPS System aber das hat beim Angriff keinen Alarm ausgelöst.
- Bei DigiNotar konnten die Angreifer sich auf jenen Systemen ausbreiten, wo keine AV Software installiert war.
- DigiNotar hat die Krise nicht gut behandelt. Weder hat man nach den ersten Hinweisen technisch richtig reagiert, noch hat die Krisenkommunikation funktioniert.
- Ersten Erkenntnissen nach wurde DigiNotar über Client-Exploits (PDF per Mail) kompromittiert. Eine harte Trennung zwischen Office-Netz und den kritischen Produktionssystemen ist (wie auch bei SCADA-Systemen) dringend nötig.
- Der Angreifer konnte seine Spuren verwischen, indem er Daten aus Logfiles löschte. Mit einer zentralen Logging Infrastruktur wäre das nicht möglich gewesen.
- Es wurde dem Angreifer viel zu leicht gemacht, die von ihm erzeugten Zertifikate nach Außen zu schmuggeln.

Weitere Informationen

Folgende Ressourcen sind gute Quellen für weitergehende Informationen zu diesem Vorfall:

GOVCERT.NL Factsheets:
https://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets

SANS Internet Storm Center:
https://isc.sans.edu/diary.html?date=2011-09-01 (Timeline)
https://isc.sans.edu/diary.html?date=2011-09-06 (Zusammenfassung des Fox-IT Reports)
https://isc.sans.edu/diary.html?date=2011-09-08

Anhang 1

Informationen laut https://isc.sans.edu/diary.html?date=2011-09-01

Folgende CAs wurden zur Erstellung von Zertifikaten missbraucht:

- DigiNotar Cyber CA
- DigiNotar Extended Validation CA
- DigiNotar Public CA - G2
- DigiNotar Public CA 2025
- Koninklijke Notariele Beroepsorganisatie CA
- Stichting TTP Infos CA

Für folgende Organisationen (Common Name, CN) wurden Zertifikate ausgestellt:

- *.*.com
- *.*.org
- *.10million.org
- *.android.com
- *.aol.com
- *.azadegi.com
- *.balatarin.com
- *.comodo.com
- *.digicert.com
- *.globalsign.com
- *.google.com
- *.JanamFadayeRahbar.com
- *.logmein.com
- *.microsoft.com
- *.mozilla.org
- *.RamzShekaneBozorg.com
- *.SahebeDonyayeDigital.com
- *.skype.com
- *.startssl.com
- *.thawthe.com
- *.torproject.org
- *.walla.co.il
- *.windowsupdate.com
- *.wordpress.com
- addons.mozilla.org
- azadegi.com
- Comodo Root CA
- CyberTrust Root CA
- DigiCert Root CA
- Equifax Root CA
- friends.walla.co.il
- GlobalSign Root CA
- login.live.com
- login.yahoo.com
- my.screenname.aol.com
- secure.logmein.com
- Thawte Root CA
- twitter.com
- Verisign Root CA
- wordpress.com
- www.10million.org
- www.balatarin.com
- www.cia.gov
- www.cybertrust.com
- www.Equifax.com
- www.facebook.com
- www.google.com
- www.hamdami.com
- www.mossad.gov.il
- www.sis.gov.uk
- www.update.microsoft.com