Security-Webinar

November 2016

Dr. Christopher Kunz, filoo GmbH

Ihr Webinar-Team

➔Referent: Dr. Christopher Kunz

- 1 / 2 Geschäftsführer filoo GmbH
- Promotion IT Security
- Vorträge auf Konferenzen
- Autor von Artikeln & Büchern

➔Moderation: Stefanie Jerchel

- Marketing Thomas-Krenn.AG
- Sammelt Fragen / Feedback

filoo GmbH

➔Hosting-Partner der Thomas-Krenn.AG

- Seit September 2016 Teil der Adacor-Gruppe
- Sicheres, hochperformantes Hosting in Frankfurt

➔Primärer Rechenzentrumsstandort Frankfurt

- Tier3, ISO 27001
- Fläche in zwei Brandabschnitten

➔Managed Services

- Planung & Deployment
- Security Services
- Systemadministration

Agenda

filoo®

➔Zertifikate, SSL und Co.

- AVM Zertifikatsprobleme
- WoSign/StartSSL Ergebnisse
- Comodo-Leseschwäche
- TLS SHA1-Sunsetting

➔Exploits

- MySQL Local Root (nochmal)
- Joomla Exploit
- Memcached

➔Nächster Termin

Ein wenig Politik

filoo®

➔Neuer Präsident in den USA

➔Trump ist kein Fan von Datenschutz

- Will Technologie-Firmen zur Datenherausgabe zwingen
- Teilnetze abschotten im Konfliktfall
- Verlängerung des „Patriot Act“
- NSA-Vorratsdatenspeicherung

➔Auswirkungen auf IT-Branche?

➔Mehr Infos: https://www.globalpolicywatch.com/2016/11/privacy-and-data-security-in-the-trump-administration/

AVM Zertifikatsprobleme

filoo®

➔Kabelnetz kennt keine Authentifizierung wie z.B. DSL

➔“nachgerüstete“ Authentifizierung von Modems im Netz

- Zertifikat enthält MAC-Adresse des Kabelmodems und ist vom Hersteller signiert
- Nur bei passenden Werten Einbuchung ins Netz möglich

➔Weiß man die MAC eines bestehenden Kunden, kann man

- Sich als dieser Kunde ausgeben
- Abhängige Subsysteme (Pay-TV, Kundenmenü, Telefonie) mißbrauchen

➔AVM speicherte privaten Schlüssel ihres Zertifikats

- ...auf Routern
- ...seit 2015
- Damit kann jeder Router-Zertifikate erstellen

WoSign / Startcom

filoo®

➔Mißtrauen für neue Zertifikate ab 21.10.16

- Apple „ab sofort“ (16.9.16)
- Chrome 56
- Firefox 51

➔Unangenehme Folgen für Auditor (Ernst&Young HK)

- Keine CA-Audits werden mehr akzeptiert

➔Startcom?

- Leitungsebene ausgetauscht
- Arbeitet an einer Lösung

➔WoSign?

- CEO entlassen
- Gibt 90% Rabatt
- Hat noch eine Intermediate CA in petto

SHA1 Sunsetting

filoo®

- ➔SHA1 als Signatur-Algorithmus ist veraltet
- ➔Trotzdem noch reichlich Zertifikate im Umlauf
- ➔Ab 1.1. werden Zertifikate mit SHA1-Signatur nicht mehr akzeptiert
  - HTTPS-Verbindungen werden unterbrochen
- ➔Gradueller Ausstieg in den ersten Jahreswochen
- ➔Prüfen Sie Ihre Zertifikate!
- ➔Unser Vertrieb macht Ihnen gern ein Angebot

Comodo kann nicht lesen

filoo®

➔Comodo-Zertifikate werden per Mail genehmigt

➔Mailadresse kommt aus whois

➔Was, wenn Whois-Server sie nur als Bild zurückliefert?

- .eu macht das, .be auch

➔Klar: OCR

➔Je nach Schrift sehen l und 1 recht ähnlich aus…

- So kann man statt info@a1telekom.at die info@altelekom.at verwenden
- …und kriegt ein Zertifikat für a1telekom.at

➔Problem seit Ende September behoben

MySQL Local Root

filoo®

- ➔Es ist alles noch viel schlimmer…
- ➔Wir erinnern uns: Root-Exploit für MySQL mit einigen Bedingungen
- ➔Durch Kombination mehrerer Lücken: Root-Zugriff mit minimalen Privilegien
  - Verzeichnisse erstellen auf dem DB-Server
  - Tabellen erstellen in einer DB
- ➔Trifft auf sehr viele Setups zu

Schritt 1: mysql-Shell erreichen

filoo®

- ➔Erstelle Verzeichnis /tmp/exploit
- ➔Permissions auf 04777 setzen (suid)
- ➔Erstelle Tabelle:
  - CREATE TABLE exploit (txt varchar(50)) engine = ‘MyISAM‘ data directory ‘/tmp/exploit‘
- ➔Tabelle lebt nun in /tmp/exploit/exploit.MYD
- ➔Kopiere /bin/bash dorthin
- ➔Sorge mittels Race Condition für passende Permissions (SUID + exec)
  - CVE-2016-6663
- ➔Führe Shell als User „mysql“ aus

Schritt 2: Root werden

filoo®

- ➔CVE-2016-6664: Race Condition im Logging
- ➔Wenn Logging in eine Datei aktiviert ist…
- ➔…tausche Logdatei schnell durch Symlink aus
- ➔Sorge dann für passende Permissions
- ➔Lade dann eine dynamische Bibliothek nach
- ➔Und werde root

Joomla

filoo®

- ➜Neue Joomla-Lücke erlaubt Account-Erstellung
  - ...und Admin-Machung
  - ...remote.
  - Ohne Genehmigung.
- ➜Details? Keine
- ➜Betroffen: 3.* < 3.6.3
- ➜Fix in 3.6.4
- ➜Automatisierte Exploits in the wild
- ➜Guide zum Joomla-Säubern: https://sucuri.net/guides/how-to-clean-hacked-joomla

Memcached remote Code

filoo®

→Verschiedene Integer Overflows

→Fehler in der SASL-Authentifizierung

→Resultat: Ausführung beliebigen Codes

→Memcached darf nie übers Internet erreichbar sein!

→Gegenmaßnahmen

- Memcached-Daemon nicht auf öffentl. IP-Adresse horchen lassen
- Aktualisierte Version 1.4.33 installieren

Neue Organisation

filoo®

➜Dies ist mein letztes Webinar bei der Thomas-Krenn.AG

➜Die Webinare werden weitergehen

➜Anmeldung für Dezember ab sofort:
https://www.filoo.de/webinar

➜E-Mail mit Aufzeichnung + Einladung

Vielen Dank!

filoo®

➜Ich freue mich auf Ihre Themenvorschläge und Fragen!

➜Kontaktdaten:

- E-Mail: chris@filoo.de
- Telefon: 05241/86730-0

➜Besuchen Sie filoo!

- https://www.filoo.de/
- http://twitter.com/filoogmbh