MUSletter

Ausgabe Februar 2018 We share Knowledge

Wenn der (elektronische) Pöstler nicht mehr klingelt

«Wotsch en Brief – so schrieb en Brief!» war ein Slogan, den man vor vielen Jahren (oder sogar Jahrzehnten?) auf den Briefkästen der Post lesen konnte. Im Grundsatz stimmt das heute noch. Aber die Art, wie wir mit unserer Umgebung kommunizieren, hat sich grundlegend verändert. Und mit diesen Änderungen kommen auch neue Probleme auf uns zu.

Auch elektronische Postfächer können überfüllt sein. *Bild: Wikipedia*

Damals – da kannte der Briefträger noch beinahe jede Person, die im Dorf oder im Quartier lebte, und die Briefe kamen auch dann an, wenn die Adresse des Empfängers unvollständig oder der Name des Empfängers an keinem Briefkasten angeschrieben war. Heute, wo der grösste Teil des Schriftverkehrs elektronisch erfolgt, geht das nicht mehr. Wenn in einer E-Mail nur ein einziger Buchstabe in der Adresse falsch ist, kann sie nicht zugestellt werden.

Es gibt aber auch Situationen, wo der Absender keine Schuld trägt, wenn eine E-Mail nicht ankommt. Zwei oft vorkommende Probleme sind Fehler beim Mailabruf (falscher Benutzername oder falsches Passwort) oder ein volles Postfach, das keine neuen Mails mehr aufnehmen kann.

Fehler beim Mailabruf

Wie beim Briefkasten vor dem Haus braucht es auch für E-Mail einen «Schlüssel», um das Postfach zu öffnen und die darin enthaltenen Mitteilungen zu lesen. Hier besteht der Schlüssel aus einem Benutzernamen und einem Passwort. Bei der MUS Mailadresse ist der Benutzername gleich wie die Mailadresse.

Bei MUS gibt es ausserdem eine Sperre – ähnlich wie beim Geldbezug am Bankautomaten: Wenn mehr als 5 falsche Anmeldungen innerhalb von 60 Minuten kommen, blockiert der Server die IP-Adresse und der Zugang ist während einer Stunde nicht mehr möglich. Wenn innerhalb dieser «Sperrstunde» weitere fehlerhafte Anmeldeversuche erfolgen, wird die Sperre dauerhaft. Dadurch soll verhindert werden, dass Unberechtigte durch x-malige Versuche Zugang zu einem Postfach erhalten. Solange die Sperre besteht, ist von dieser IP-Adresse kein Zugang mehr zum Postfach möglich. Und auch die MUS-Webseite <http://www.mus.ch> ist nicht mehr erreichbar.

Um die Sperre wieder aufzuheben schreibt man am besten (von einer anderen Mailadresse aus) eine Nachricht an <webteam@mus.ch> mit Angabe der betroffenen Mailadresse und der eigenen IP-Adresse. Zur Feststellung der IP-Adresse genügt es, im Browser <http://wieistmeineip.de> aufrufen. Wir brauchen die IPv4 Adresse, die sich aus 4 Zahlengruppen im Format von 123.123.123.123 zusammensetzt.

Volles Postfach

Die von MUS zur Verfügung gestellte Mailadresse hat eine Kapazität von 250 MB. Sobald sich das Postfach zu

sehr füllt bekommt der Benutzer eine automatisch generierte Information, dass die Kapazitätsgrenze bald erreicht sein wird. Dann ist «aufräumen» angesagt! Nicht mehr benötigte Mails können natürlich problemlos gelöscht werden um Platz zu schaffen. Aber was macht man mit den Nachrichten, die eventuell noch gebraucht werden?

Wer IMAP für das MUS-Postfach verwendet, kann im Mailprogramm einen lokalen Ordner anlegen und die Nachrichten dorthin verschieben. Dadurch werden die Nachrichten auf dem Server gelöscht und sind nur noch im lokalen Postfach vorhanden. Wenn die Nachrichten auf mehreren Geräten noch gespeichert bleiben sollen, kann man das lokale Postfach danach exportieren und woanders wieder importieren.

Auch hier gilt: Wer Probleme hat mit dem MUS-Postfach kann sich mit seinen Fragen an <webteam@mus.ch> wenden.

Christian Buser

Wurden deine Daten schon ausspioniert?

Täglich werden auf verschiedenen online Plattformen persönliche Identitätsdaten durch Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird an interessierte Kreise verkauft oder in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere Angriffe. Siehe dazu auch den Artikel im Januar Falter und Pauls Erfahrungsbericht auf der nächsten Seite.

Das Hasso-Plattner-Institut der Universität Potsdam stellt mit dem «HPI Identity Leak Checker» ein Werkzeug zur Verfügung mit dem du prüfen kannst, ob deine persönlichen Identitätsdaten bereits im Internet kursieren. Es kontrolliert, ob deine E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

Die Benutzung ist ganz einfach: Auf https://sec.hpi.de/ilc/search gibst du deine E-Mail Adresse ein und Sekunden später erhältst du auf diese Adresse ein E-Mail mit den gefundenen Angaben. Das sieht im Idealfall z.B. so aus:
Glückwunsch: Ihre E-Mail-Adresse werner@mus.ch taucht nicht in unserer Datenbank auf. Das garantiert jedoch nicht, dass keine Ihrer persönlichen Informationen gestohlen wurden.

Leider gibt es aber auch diese Variante:

Betroffener Dienst	Datum	Verifiziert	Passwort	Vor- und Zuname	Geburtsdatum
adobe.com	Okt. 2013	✓	Betroffen	-	-

Da hat Adobe mit meinen Daten geschlampt! *Werner Widmer*

LocalTalk Basel

Nächster LT Termin
8. Februar 2018, 19 Uhr. Apéro bis 19.30 Uhr.

Thema
Apple und die CPU Lücken.

Ort
Gruner AG, Citygate (Gebäude C), Auditorium, St. Jakobs-Strasse 199, 4052 Basel.

Weitere Infos
http://www.mus.ch/lt-basel
ekuchinka@yahoo.com

Auf zahlreiches Erscheinen freuen sich
Ellen Kuchinka und Pit Hänger

LT Bern / Luzern

http://www.mus.ch/lt-bern

Christian Zuppinger,
czuppinger@bluewin.ch

http://www.mus.ch/lt-luzern

Adrian Reichmuth
http://www.reichmuth-informatik.ch

LocalTalk Zürich

(macht derzeit Pause)

Infos unter sekretariat@mus.ch

Stellenabgebot

EDV-Supporter/in (Mac) 50%

gesucht für das Deutsche Seminar der Universität Zürich, per 01.03.2018 oder nach Vereinbarung.
Bewerbungsfrist bis 2.2.2018!
Details zur Ausschreibung hier:
http://www.jobs.uzh.ch/jobDetail.php?jobID=7900

Neulich im IT Support

Werners Tipps und Tricks

Neu gekaufter iMac gesperrt. Die Wegelagerer des 21. Jahrhunderts sind da!

Im Januar 2018 erschien im MUS Falter unter dem Titel «Wie mein iMac gestohlen wurde» ein Bericht über Apple Geräte, welche von Hackern gesperrt worden waren. Paul Hösli, ehemaliges MUS Vorstands-Mitglied, hat exakt das Gleiche am eigenen Leib erfahren - und zwar bereits im letzten Sommer. Hier sein Bericht.

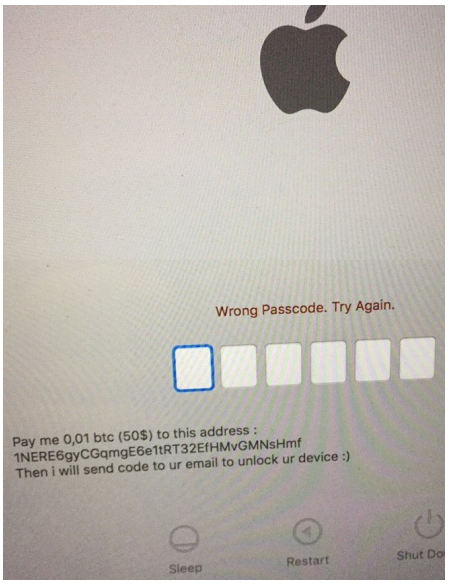
Am 11. Juli 2017 liess ich beim Hasso-Plattner-Institut der Universität Potsdam mittels Identity Leak Checker auf <https://sec.hpi.de/leak-checker/search> meine E-Mail Adresse überprüfen. Und erhielt prompt die Auskunft, dass meine Mail-Adresse in mindestens einer gestohlenen und unrechtmässig veröffentlichten Identitätsdatenbank auftaucht. In der WHOIS-Database der NET-Domains bin ich mit Vor- und Zunahme aufgeführt. Diese Daten wurden im März 2017 von Hackern gestohlen.

Betroffener Dienst	Datum	Verifiziert	Passwort	Vor- und Zuname
WHOIS Database (NET-Domains)	Mär. 2017	✓	-	Betroffen
adobe.com	Okt. 2013	✓	Betroffen	-
dropbox.com	Sep. 2012	✓	Betroffen	-

Andere Diebe hatten sich schon im Oktober 2013 bei adobe.com bedient. Und bei dropbox.com waren bereits im September 2012 E-Mail Adressen und Passwörter gestohlen worden. Bei beiden war ich mit der E-Mail Adresse, bestehend aus Vor- und Nachnamen, drin. Kein Problem, das Dropbox-Passwort hatte ich ja kürzlich geändert. Dachte ich.

Am Freitag, 21.7.2017 holte ich meinen neuen iMac ab und nahm ihn tags darauf probeweise in Betrieb. Anmeldung bei iCloud und Dropbox-Anmeldung habe ich gleich gemacht. Am Sonntag schien am Anfang alles gut zu laufen. Dann installierte ich einige Programme. In kurzer Zeit wurde der iMac von Meldungen des Systems, von Programmen und von Little Snitch so überflutet, dass ich zeitweise 15 Abfragen und Meldungen gleichzeitig auf dem Desktop hatte und nach dem Wegklicken oft gleich drei neue hinzu kamen.

Ich sah aus dem Augenwinkel eine Bewegung nach links, die ich mir nicht erklären konnte - und schon lief es ab: Kurz darauf erschien eine Passwort-Abfrage vom Mac. Die Passworteingabe wurde mit Schütteln quittiert. Ich versuchte es noch zweimal und verstand nicht, wieso mein Passwort nicht angenommen wurde. Dann die Meldung, ich solle es in 5 Minuten wieder probieren. Unter der Codezeile für das Passwort erschien eine Mailadresse an die man schreiben konnte.



Bald darauf kam eine Meldung von iCloud: «Dieser Mac wurde am 23. Juli 2017 um 08:38 Uhr PDT gesperrt. Wenn du wieder im Besitz deines Mac bist, entriegle ihn mithilfe des Codes, den du beim Sperren deines Mac eingerichtet hattest.» Ich meldete alle Geräte in iCloud ab, setzte das Passwort für meine Apple-ID zurück und änderte es sofort wieder.

Danach folgte der Gang zu Apple an die Bahnhofstrasse. Dort wurde der iMac innert einer Stunde kostenlos freigeschaltet. Alle Daten waren natürlich weg, neu installieren war angesagt. Für die Entschlüsselung der Geräte wird ein Kaufnachweis mit der Geräte-Seriennummer und ein persönlicher Ausweis verlangt.

Ein gesperrtes iOS-Gerät freischalten ist einfacher - vorausgesetzt man kann es in iCloud abmelden. Und hat schon mal mit iTunes ein Backup gemacht. Gerät einfach an iTunes anschliessen und mittels der Funktion «iPhone wiederherstellen» auf den Fabrikzustand zurücksetzen. Dann das Backup wieder einspielen.

Falls iTunes das iOS-Gerät nicht erkennt klappt die Rücksetzung auf den Auslieferungs-Zustand nicht. In diesem Fall bleibt nur der Gang zu Apple oder einem AASP (Apple Autorisierter Service Provider).

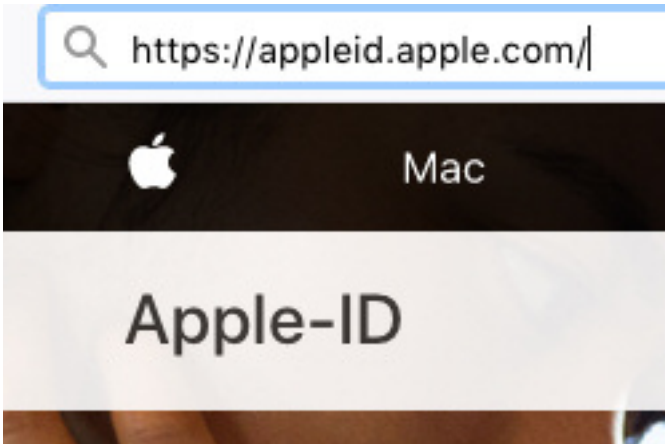
Tipp: Wenn du dein iCloud-Passwort schon länger nicht mehr geändert hast wäre jetzt der richtige Zeitpunkt dazu.

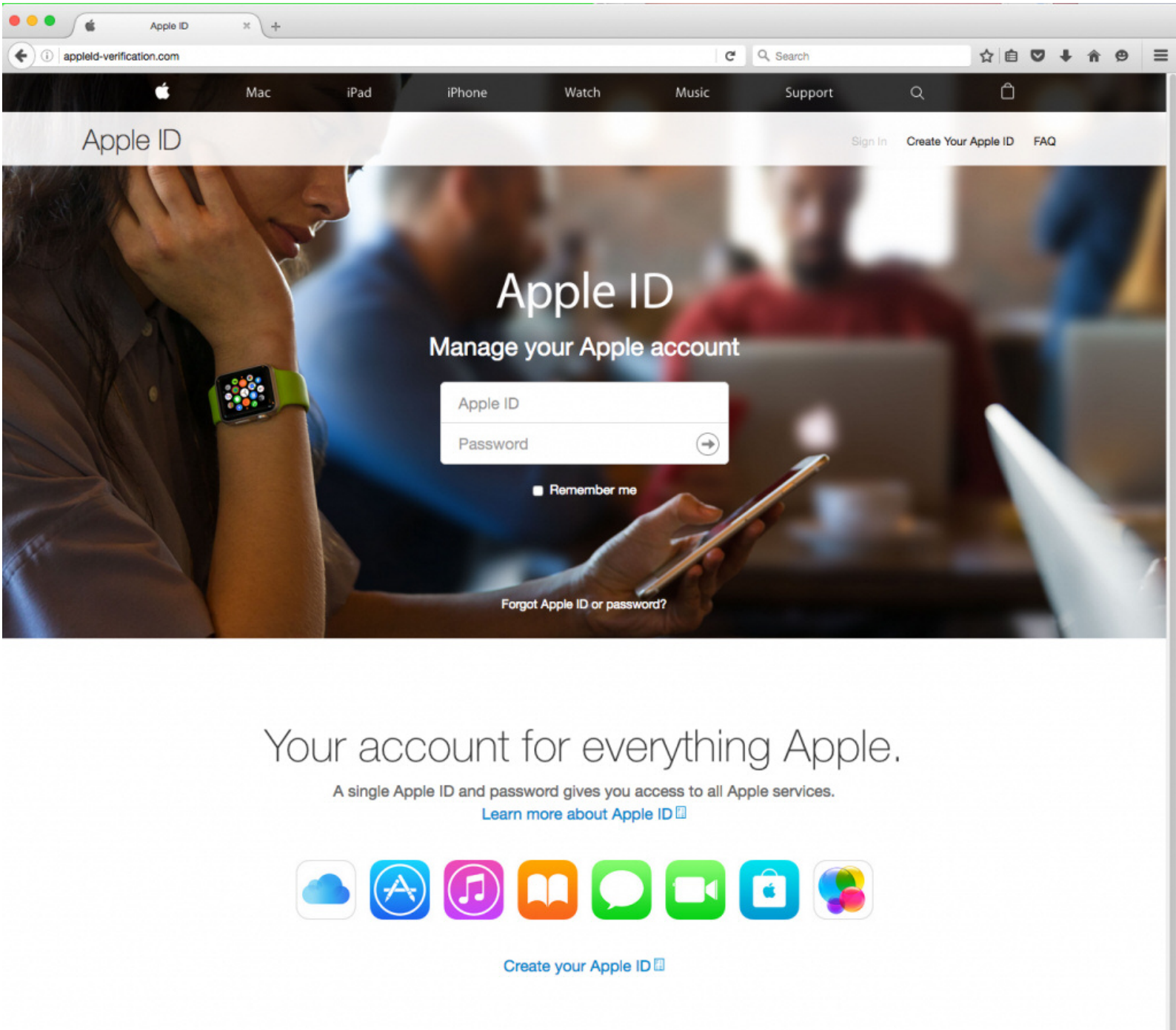
Wie der Hack funktioniert kannst du bei Apple unter dem Titel «Firmware-Passwort für einmalige Nutzung festlegen» nachlesen: <https://support.apple.com/de-de/HT204455>

Paul F. Hösli

Nicht immer werden die Daten von schlecht gesicherten Webseiten gestohlen. Manchmal ist man einfach unvorsichtig und gibt seine Daten freiwillg in falsche Hände. «Phishing» ist eine beliebte Methode, um an Benutzerdaten zu kommen. Einige dieser Phishing Seiten sind so täuschend echt nachgebaut, dass sie kaum von der echten Seite zu unterscheiden sind. Im vorliegenden Beispiel sind alle Links innerhalb der Seite korrekt und verweisen auf die echten Apple Seiten. Nur die Felder AppleID und Passwort nicht. Sie liefern die Daten geradewegs den Hackern in die Finger.

Die URL-Zeile verrät den Betrug:
<appleid-verification.com> ist eine Phishing Seite.
<https://appleid.apple.com>ist die echte Seite





Apple und Intel – vertuschen oder schönreden bringt nichts

Mit viel PR versuchten Apple und Intel zum Jahreswechsel die Wogen der iPhone-Akku-Affäre sowie der Meltdown- und Spectre-Sicherheitslücken zu glätten. Beide Konzerne erwischten einen denkbar schlechten Start ins neue Jahr und wurden mit etlichen Negativschlagzeilen auf dem falschen Fuss erwischt.

Eigentlich wollte Apple nur das Beste für seine Kunden. Um die alternden Akkus der iPhones zu schonen, reduzierte man klammheimlich die Leistung des Prozessors. Zu dumm, dass findige Köpfe durch Benchmarks den Nebeneffekt aufdeckten.

Vollständige Versionshinweise von Software gehören eigentlich zur Produktqualität. Nur komisch, dass Cupertino erst auf massiven Druck – wie leider in der Vergangenheit üblich – reagierte und den Akkuaustausch praktisch verschenken muss. Tim Cook gestand: «Hätten vielleicht klarer sein können». Ehrliche Kommunikation zur richtigen Zeit ist alles. Anstelle von «verbessert die Stabilität, Zuverlässigkeit und Sicherheit» sollte mehr Fleisch am Knochen sein. Mit iOS 11.3 soll übrigens der Kunde die Drosselbremse bei schwachem iPhone-Akku abschalten können. Ein neuer Akku ist auf jeden Fall besser.

Intels Sicherheitslücke bei fast allen Prozessoren seit 2008 war ein Knaller. Andreas Stiller von der Heise-Redaktion sprach vom Security-Supergau. Um sich aus dem Schlamassel zu befreien, verkündete der Monopolist, dass «alles so funktioniere wie es designt wurde», und zeigte gleichzeitig mit dem Finger auf die Konkurrenz wie AMD und ARM.

Und überhaupt würde der Anwender mit den geplanten Updates für Betriebssystem, Browser und BIOS bloss minimale Leistungseinbussen im Alltag bemerken. Dafür, dass Intel seit einem halben Jahr von den Schwachstellen in der Hardware-Architektur seiner Prozessoren wusste, herrschte bei Angaben zu den betroffen Chips und Bug-Fixes das nackte Chaos. Obendrein führten die Mikrocode-Aktualisierungen vereinzelt zu Problemen auf Windows- und Linux-Rechnern, und mussten zurückgerufen werden.

Intel CEO Brian Krzanich verkaufte so viele Aktien des Unternehmens, wie er konnte. Zufall oder Absicht? Die Intel-Kunden warten weiter auf Lösungen für Meltdown und Spectre.

Apple hatte seine Hausaufgaben gemacht und lieferte Updates gegen die Prozessorlücken für iOS 11 und die letzten drei Mac OS Versionen. Trotzdem bleiben viele Apple-Geräte mit älteren Systemen weiterhin ungeschützt. Als Kunde fühlt man sich schon veräppelt und sitzt nach der Installation gefühlt vor einer langsameren Kiste. Der Performanceverlust beträgt je nach Fall von wenigen bis zu 30 Prozent. 2018 beginnt spannend und die Anwälte werden sicher nicht arbeitslos.

Apfelbeisser

044 915 77 66

Kostenlose Unterstützung für MUS-Mitglieder

Sie möchten Mitglied werden? Rufen Sie die Nummer der Helpline an – sie hilft auch in solchen Fällen!

MUS GV 2018

Datum
26. Mai 2018, ca. 10 bis 16 Uhr.

Ort
Bern

Weitere Infos
folgen im nächsten MUSLetter. Reserviere dir schon mal das Datum!

MUS Workshop

Datum
Freitag 13. April 2018, 19 Uhr und Samstag 9. Juni 2018, 14 Uhr.

Ort
Berglistrasse 6, 8703 Erlenbach

Thema
Wie bringe ich meine Musik in guter Qualität von meinem Mac oder iOS Gerät auf die Lautsprecher? Alles was du schon immer wissen woltest über Streaming, AirPlay, MP3, AAC, Lossless, AIFF, FLAC, SACD, DSD usw. Du hast die Gelegenheit, verschiedene Formate auf HighEnd Anlagen (Denon, Monitor Audio, Mission, Piega, Technics) zu vergleichen.