Defensive Con @ c-base

Defensiv statt Offensiv!

Manuel (HonkHase) Atug

Über mich
Manuel (HonkHase) Atug

- Senior Manager bei der HiSolutions AG
- Diplom-Informatiker & Master of Science in Applied IT Security
- seit über 20 Jahren in der Informationssicherheit tätig
- Spezialthemen: KRITIS und Ethik

Seit bis zu ~20 Jahren Aktiv in so n paar Vereinen:

- Chaos Computer Club e.V., Chaos Computer Club Cologne e.V., c-base e.V.
- Digitale Kultur e.V., ISACA, GI e.V., FIfF e.V., Freie Software Freunde e.V

AGENDA

1. Warum Defensive Con?
2. Wünsch Dir was!
3. Wieso Defensiv statt Offensiv am Beispiel von KRITIS
4. Und nun?

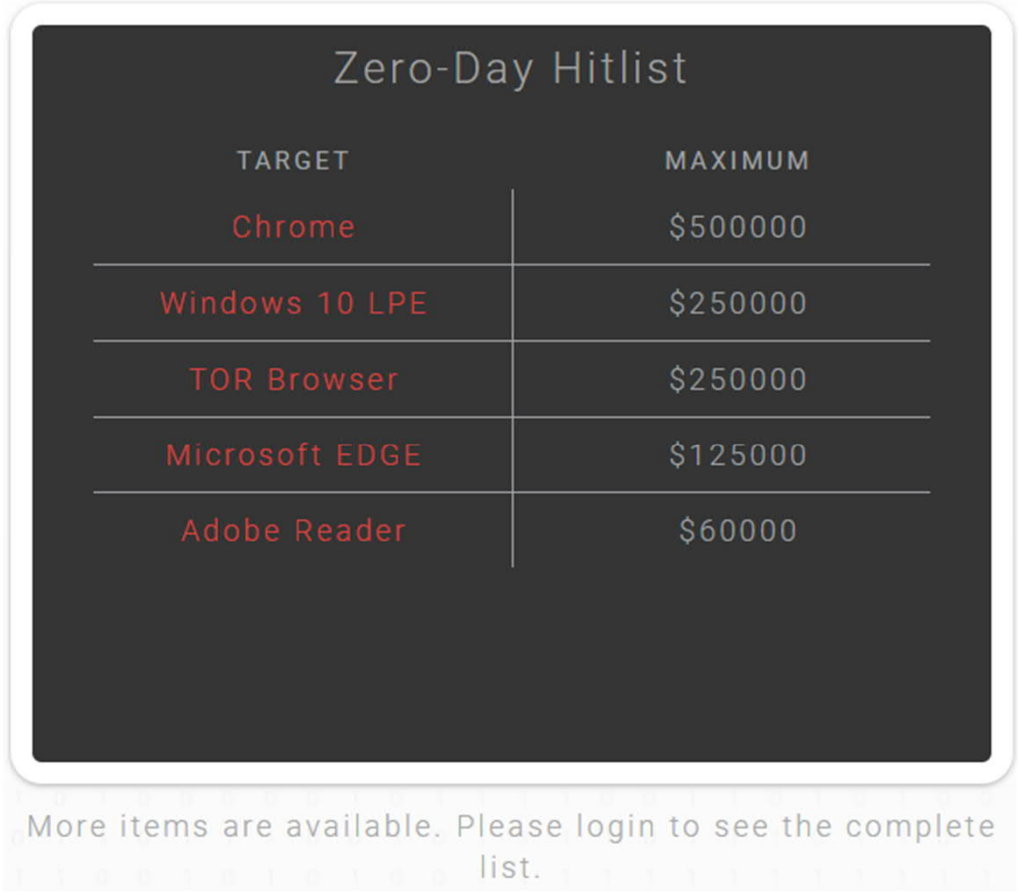
1. Warum Defensive Con?

Wie alles halt so anfängt…

- 2018 gab es eine Offensive Con in Berlin, die ich verschmäht hatte! Geht ja garnicht!!!eins!!elf!!
- Teilnehmer berichteten von 0day-Händlern vor Ort und den Marktpreisen für „Government“
- Ich wollte mir ein eigenes ethisches Bild in 2019 machen… habe aber kein Ticket erhalten.

Un wat nu?
Mit Geraffel, c-base und anderen Defensiv diskutieren statt Offensiv zu beobachten!

Preisliste Exodus Intelligence - Zero-Day Hitlist



Exodus Intelligence Zero-Day Hitlist https://rsp.exodusintel.com

Preisliste von Zerodium

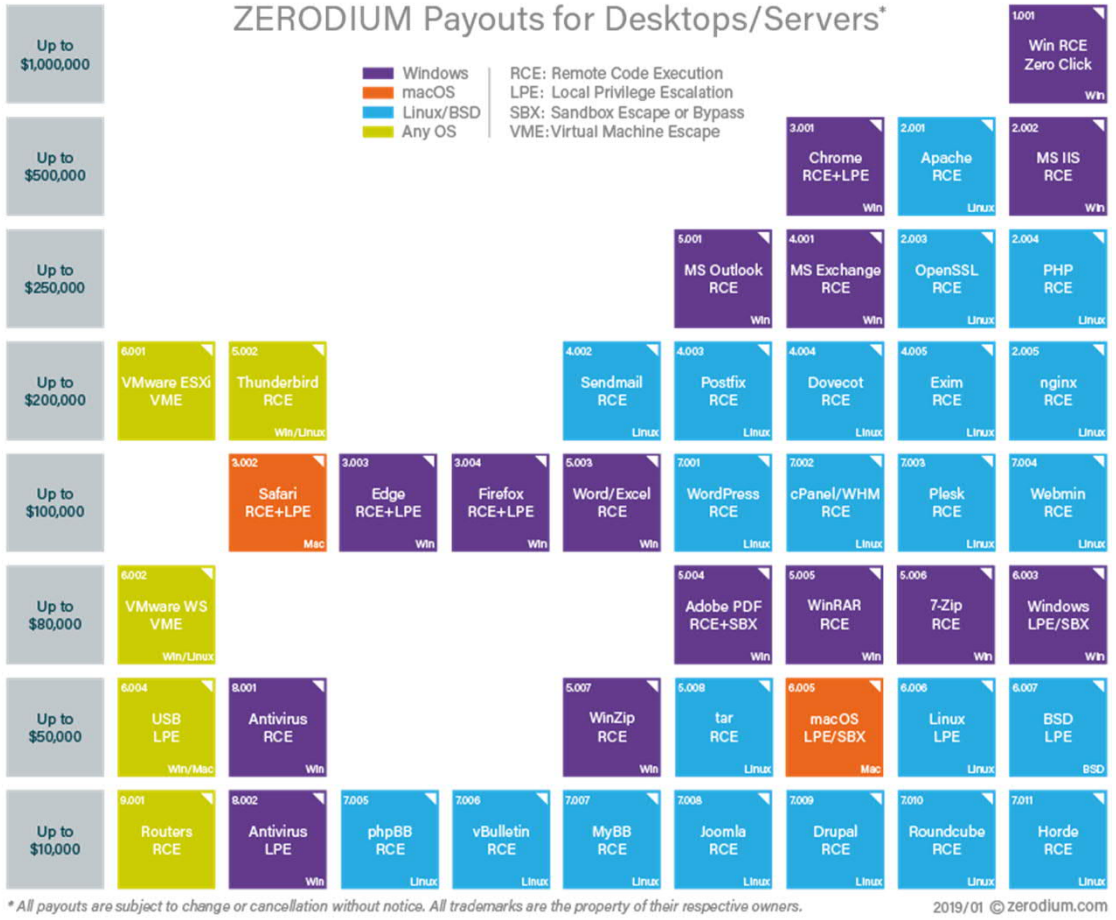
New Payouts Highlights

Jan. 7, 2019 - Payouts for the majority of Desktops/Servers and Mobile exploits have been increased. Major changes are highlighted below:

Modification	Details
Increased Payouts (**Mobiles**)	**$2,000,000** - Apple iOS remote jailbreak (Zero Click) with persistence (previously: **$1,500,000**) **$1,500,000** - Apple iOS remote jailbreak (One Click) with persistence (previously: **$1,000,000**) **$1,000,000** - WhatsApp, iMessage, or SMS/MMS remote code execution (previously: **$500,000**) **$500,000** - Chrome RCE + LPE (Android) including a sandbox escape (previously: **$200,000**) **$500,000** - Safari + LPE (iOS) including a sandbox escape (previously: **$200,000**) **$200,000** - Local privilege escalation to either kernel or root for Android or iOS (previously: **$100,000**) **$100,000** - Local pin/passcode or Touch ID bypass for Android or iOS (previously: **$15,000**) NOTE: Payouts were also increased for other products including: RCE via documents/medias, RCE via MitM, ASLR or kASLR bypass, information disclosure, etc.
Increased Payouts (**Servers/Desktops**)	**$1,000,000** - Windows RCE (Zero Click) e.g. via SMB or RDP packets (previously: **$500,000**) **$500,000** - Chrome RCE + SBX (Windows) including a sandbox escape (previously: **$250,000**) **$500,000** - Apache or MS IIS RCE i.e. remote exploits via HTTP(S) requests (previously: **$250,000**) **$250,000** - Outlook RCE i.e. remote exploits via a malicious email (previously: **$150,000**) **$250,000** - PHP or OpenSSL RCE (previously: **$150,000**) **$250,000** - MS Exchange Server RCE (previously: **$150,000**) **$200,000** - VMWare ESXi VM Escape i.e. guest-to-host escape (previously: **$100,000**) **$80,000** - Windows local privilege escalation or sandbox escape (previously: **$50,000**) NOTE: Payouts were also increased for other products including: Thunderbird, VMWare Workstation, Plesk, cPanel, Webmin, WordPress, 7-Zip, WinRAR, etc.

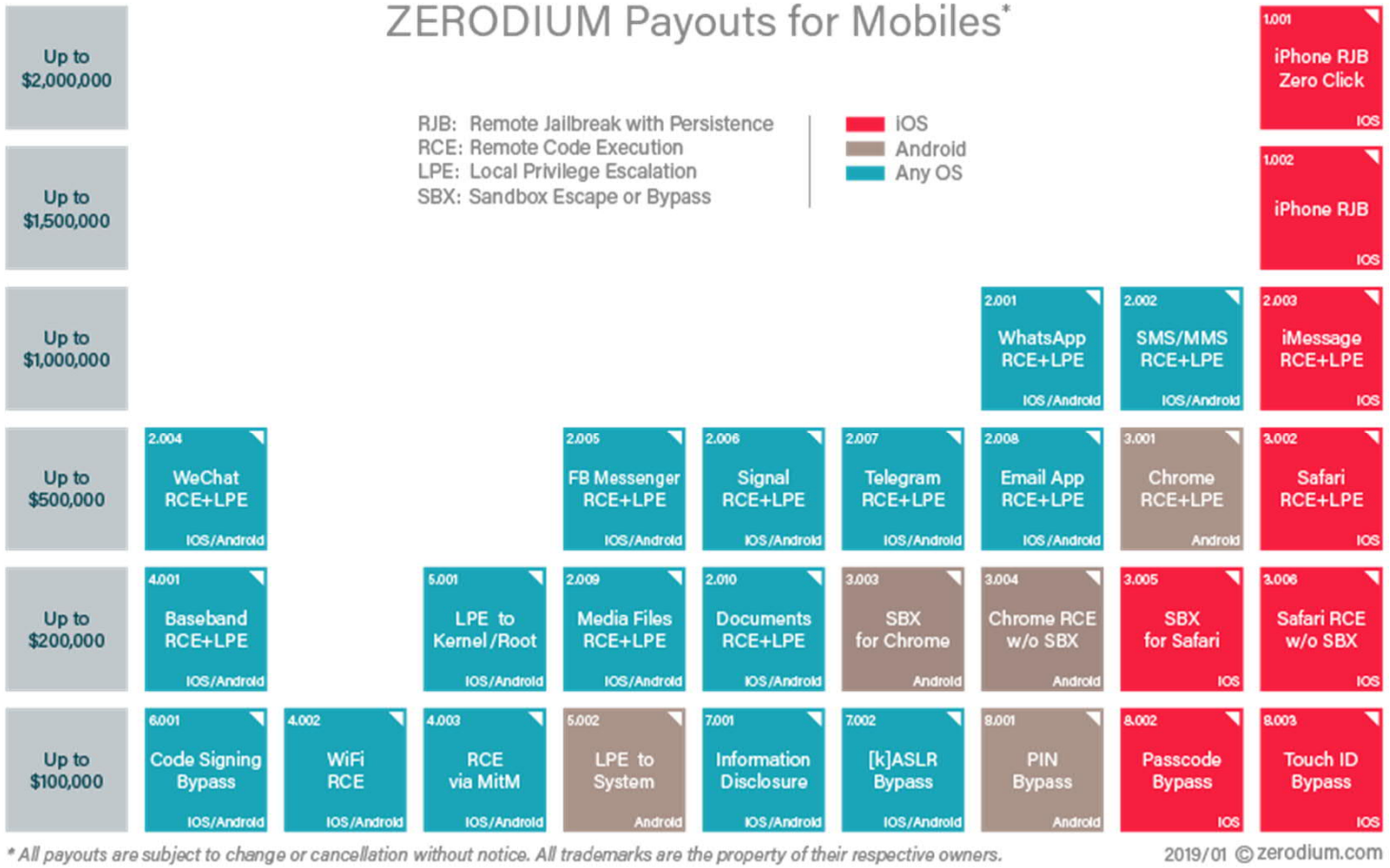
Zerodium Hit List https://www.zerodium.com/program.html

Preisliste von Zerodium - Desktop / Server



Zerodium Hit List (Desktop / Server) https://www.zerodium.com/program.html

Preisliste von Zerodium - Mobiles



Zerodium Hit List (Mobiles) https://www.zerodium.com/program.html

2. Wünsch Dir was!

Legal? Illegal? Sch...egal?!?

Marktpreise für 0days sind nicht zu unterschätzen, Staaten feuern den Markt an

4 Mio wurden dem BKA bereitgestellt, um 0days kaufen zu dürfen

BKA bezahlte knapp 6 Millionen Euro für Staatstrojaner

Schon vor zehn Jahren hat das BSI dem Bundeskriminalamt bei der Programmierung eines Staatstrojaners geholfen und Quellcode beigesteuert

Das BKA besitzt mittlerweile gleich drei einsatzbereite Staatstrojaner

Nö, wir wünschen lieber, dass sowas nicht legal gehandelt werden darf!

https://netzpolitik.org/2018/it-sicherheit-das-bka-verhindert-dass-sicherheitsluecken-geschlossen-werden/

Vulnerabilities Equities Process? Nein Danke!

Neueste Forderung vom BMI

- Andreas Könen, Abteilungsleiter im BMI wünscht:
  dass der Staat 0days horten darf und
  einen Vulnerabilities Equities Process nach US-Vorbild aufsetzt

- Die Stiftung Neue Verantwortung singt im Lied fröhlich mit:
  Schwachstellen-Management für mehr Sicherheit
  Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte

Nö, wir wünschen lieber die Ächtung digitaler Waffen!

3. Wieso Defensiv statt Offensiv am Beispiel von KRITIS

KRITIS in Deutschland

- Primärziel: Vermeidung von Versorgungsengpässen für die Gesamtbevölkerung
- Ansatz: Sicherheit der IT-Komponenten von kritischen Infrastrukturen
- Rechtlich verbindlich ab einer Versorgung von mindestens 500.000 Bürgern
- Sektoren aktuell: Energie, IT & TK, Transport & Verkehr, Gesundheit, Wasser, Ernährung, Finanzen & Versicherungen

Attacken auf das Ukrainische Stromnetz

Zielgerichtete Angriffe auf die Stromversorgung

- Dezember 2015
- Wiederholte Attacke im Dezember 2016
- Auswirkungen: ca. 250.000 betroffene Personen in Kiew und dem Umfeld

Firmware der Stromunterbrecher wurde gezielt manipuliert

Cyber-Angriffe auf deutsche Energieversorger

2017 und 2018 erfolgte eine Reihe großangelegter weltweiter Cyber-Angriffskampagnen

Cyber-Angriffe

- Deutsche Unternehmen aus der Energiebranche waren und sind 2017 und 2018 das Ziel von großangelegten weltweiten Cyber-Angriffskampagnen.

- Laut BSI liegen derzeit keine Hinweise auf erfolgreiche Zugriffe auf Produktions- oder Steuerungsnetzwerke vor. Es sei nur eine Frage der Zeit, bis neue, erfolgreiche Angriffe ausgeübt würden.

Daher müsse man das IT-Sicherheitsgesetz fortschreiben

Hacken der Bundesregierung

Es wurden Daten exfiltriert und eine Schadsoftware wurde eingeschleust

Die Attacke wurde erst im Dezember 2017 erkannt, obwohl der Angriff bereits seit einem Jahr lief

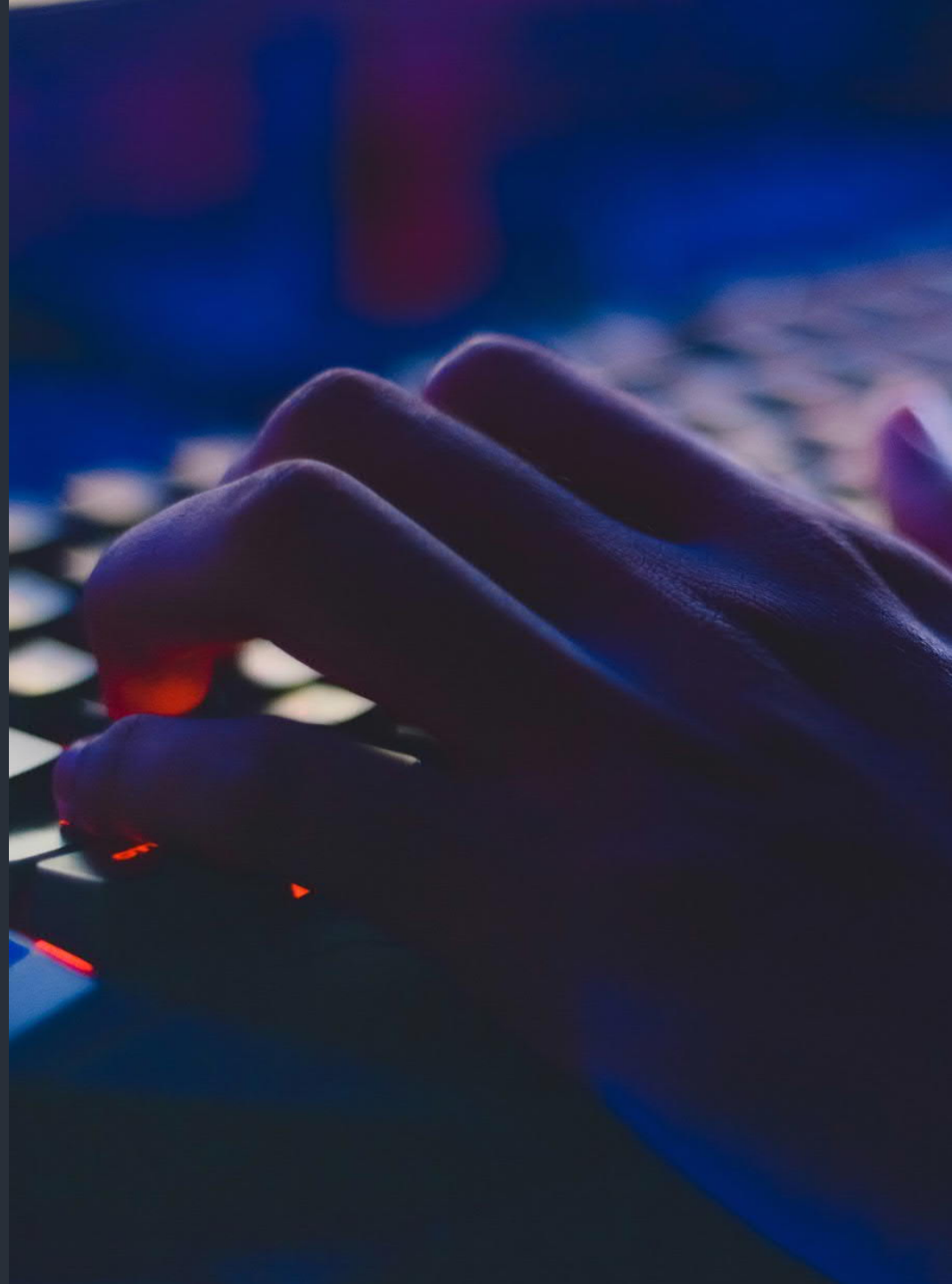
Weitere Angriffe und Ausfälle in 2018

Angriffe:

- US-Krankenhaus von Ransomware teilweise lahmgelegt

Ausfälle:

- Schwere Computerpanne am Frankfurter Flughafen
- USV Ausfall bei einem deutschen Hoster
- Computerausfall der europäischen Flugsicherung Eurocontrol
- Belgischer Luftraum durch technische Probleme gesperrt
- Kfz-Zulassung in ganz Deutschland ausgefallen
- Flugbetrieb in Hamburg nach Stromausfall eingestellt



KRITIS Defensiv statt Offensiv!

- KRITIS dient primär dem Schutz der Bevölkerung, nicht des Betreibers.
- Kritische Infrastrukturen setzen oftmals identische Komponenten ein
- Immer mehr Komponenten werden an das Internet verbunden
- Durch den Staat zurückgehaltene 0day Lücken in Kritischen Infrastrukturen bedrohen die Bevölkerung!

4. Und nun?

Schlussfo[lge|rder]rung (1/2)

- Strikt defensive Cybersicherheitsstrategie für den deutschen Staat
- Ächtung von ABCD-Waffen (inkl. Digitalen Waffen)
- Unabhängigkeit des BSI vom BMI

Schlussfo[lge|rder]rung (2/2)

Strikt defensive Cybersicherheitsstrategie für Deutschland!

- Im KRITIS-Umfeld eingesetzte Software grundsätzlich als Open Source oder Quellcode in treuhänderischer Verwaltung
- Keine Bereitstellung von Budgets für Behörden, Dienste und Agenturen, um 0days kaufen zu dürfen
- Verpflichtung für alle Behörden, Dienste und Agenturen, ihnen bekannt gewordene Schwachstellen über das BSI an den Hersteller zu melden
- BSI wie den Bundesbeauftragten f. Datenschutz direkt dem Bundestag unterstellen?
  Rechtsaufsicht -> BMI, Fachaufsicht -> BSI?
  Fach- und Rechtsaufsicht lassen sich nämlich teilen. Demokratisch.

Was ihr mitnehmen solltet:

1. Wir wollen eine strikt defensive Cybersicherheitsstrategie für Deutschland
2. Wir wollen keine ABCD-Waffen, auch nicht unter dem Deckmantel Staatstrojaner
3. Bevölkerungsschutz fängt bei der Kommunikation vorhandener Schwachstellen an den Hersteller

Kontaktdaten:

HonkHase

honkhase@blablasecurity.de |
+49 555 FTWTFCYBERWEHR

www.honkhase.de |
www.blablasecurity.de

„Fünf Minuten vor der Party
ist nicht die Zeit, um
tanzen zu lernen.“