



2016 – Das Jahr der Ransomware Trojaner PowerShell und der 2. Frühling von Office Macros

Sebastian Brabetz,
Teamleiter Professional Security Solutions
mod IT GmbH

Vorstellung Sebastian Brabetz

30 Jahre alt

Seit 2,5 Jahren bei mod IT

Seit Januar 16 Teamleiter Professional Security Solutions

Vorher bei produzierenden Unternehmen in Kassel:

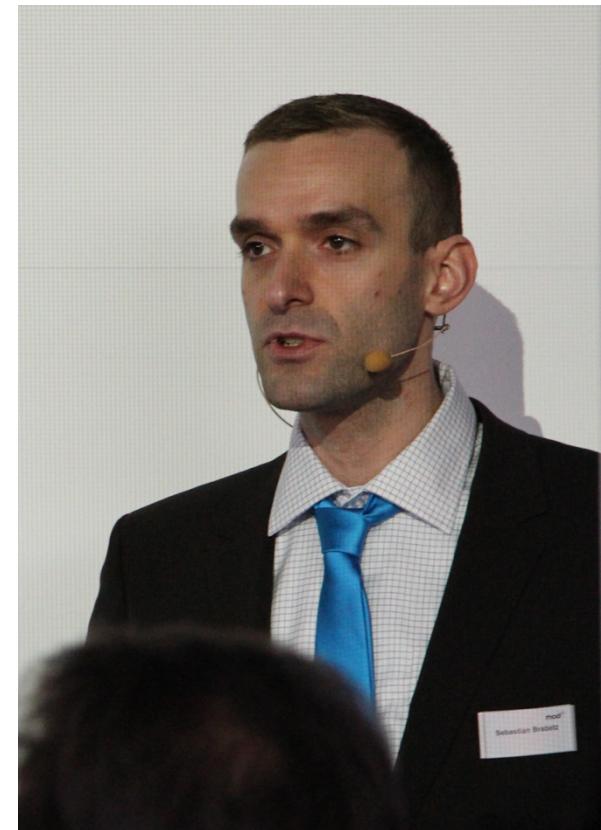
Ausbildung -> Firewall Admin -> Security Admin

Schwachstellenscans, Schwachstellenmgmt, Pentests

OSCP+TCSE Zertifiziert

Community:

- [Kassel Codemeetup](#) (Vorträge)
- [IT Security Meetup Kassel + Nordhessen](#) (Organisator)
- Metasploit Workshops
- uvm.: siehe <https://itunsecurity.wordpress.com>





All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC \approx 550 USD.

Your Bitcoin address for payment: 3t3sp9wF299y4L21uHACdUeL3Q9

\$ PURCHASE PRIVATE KEY
WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)

Message des Vortrags 1/2 – Keine Magische Lösung!

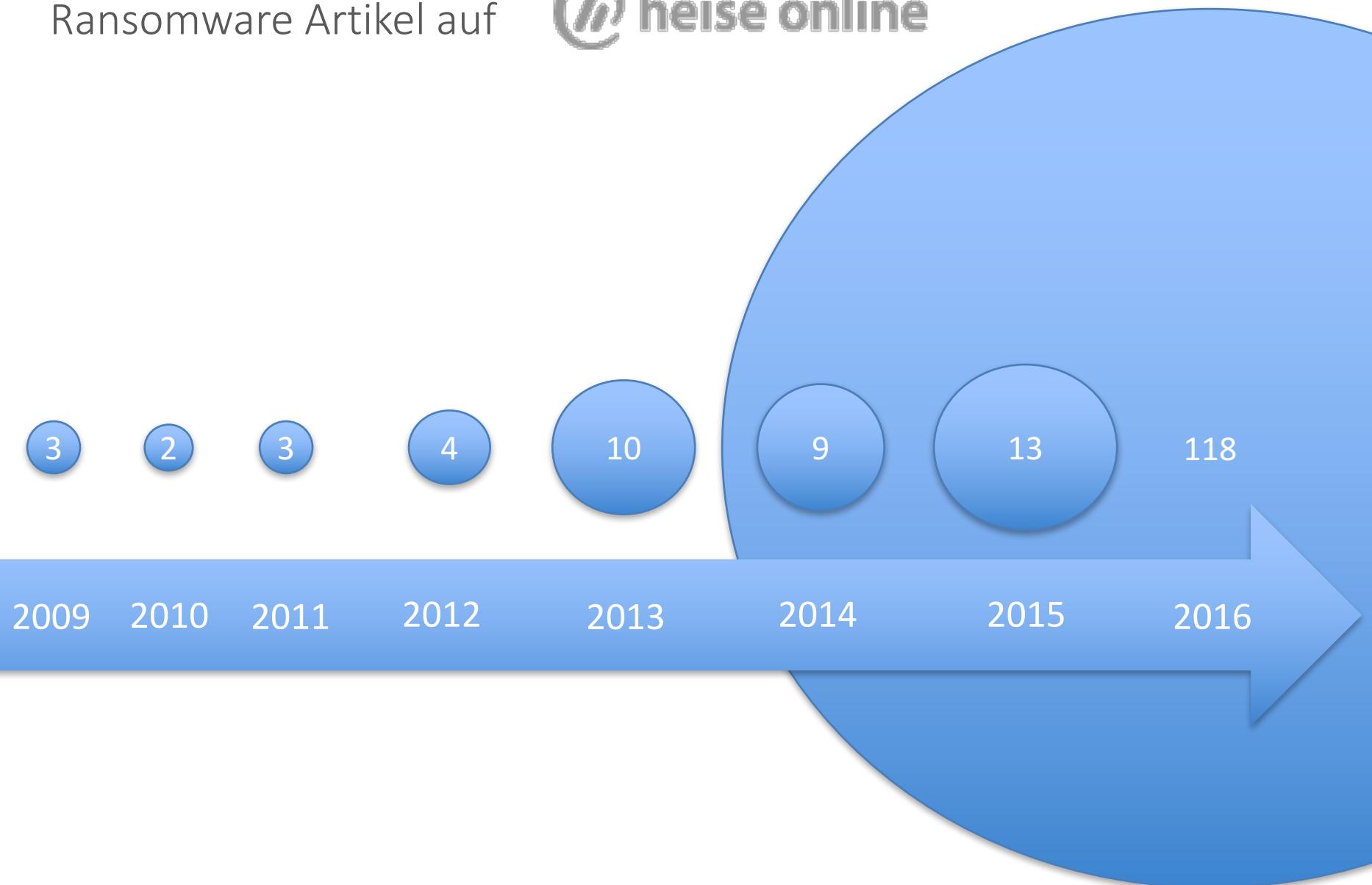
- Keine Anleitung zum Schutz von Ransomware
- Es gibt kein 19“ Rackmount / Allheilmittel von der Stange!
- Es hilft nur PPT:
 - People → Qualifiziertes Personal...
 - Processes → ...mit den richtigen Prozessen...
 - Technology → ...kann Tools zur Unterstützung einsetzen!

Message des Vortrags 2/2 – Aufklärung!

- Qualität und Aggressivität von Ransomware eskaliert
- Alte Verbreitungstechniken leben neu auf
- Klassische Security-Tools werden umgangen
- Moderne Angreifer nutzen Boardmittel

- Awareness für das Thema und die Gefahren schaffen
- Und Sie Unterhalten...

Ransomware Artikel auf



Auch unsere Kunden waren betroffen!

POLIZEIINSPEKTION NORTHEIM/OSTERODE

POL-NOM: Internetkriminalität - Polizei warnt Firmen vor Trojanern

06.06.2016 – 16:01

Northeim (ots) - NORTHEIM (fal/reit) - Nachdem in der Vergangenheit meist Privatpersonen Opfer von Ransomware-Attacken wurden, haben Cyberkriminelle jetzt zunehmend auch kleinere und größere Firmen im Visier. Aktuell sind die Ransomware-Trojaner "Petya" und "Cerber" im Umlauf.

Eine Firma aus Einbeck war in den vergangenen Tagen Ziel der Kriminellen. Den Betrieb erreichte eine E-Mail mit einem Worddokument als Dateianhang. Die E-Mail war als "Bewerbung" getarnt. Nach dem Öffnen des Dateianhangs lud sich im Hintergrund eine Schadsoftware nach. Glücklicherweise wurde der Vorfall rechtzeitig bemerkt. Umgehend wurden alle Personal Computer daraufhin für mehrere Stunden ausgeschaltet und vom Netz genommen. **Mit Hilfe einer sofort hinzugezogenen IT-Firma konnte größerer Schaden verhindert werden.** Dennoch entstanden der Firma Kosten in Höhe von ca. 10.000 Euro.

Direktes Feedback Polizei Niedersachsen:

"Für die hervorragende Zusammenarbeit und die professionelle Aufbereitung der von Ihnen festgestellten Ermittlungsergebnisse möchte ich mich nochmals ausdrücklich bedanken."

*„Was ist eigentlich so schlimm
daran wenn ein einzelner
Computer verschlüsselt wird?“*

Was ist eigentlich so schlimm daran...



- Meistens Nichts!
- Bis die Ransomware komplette Netzlaufwerke verschlüsselt!

- Wie weit geht ihre Backupkette zurück? - (VTL?)
- Konsistenz von Daten?

- Was ist wenn sie beim Jahresabschluss feststellen, dass wichtige Daten verschlüsselt wurden und es keinem aufgefallen ist?

Zahlen oder doch nicht?

Empfehlung des FBI: Bei Erpressungs-Trojanern klein beigeben und einfach bezahlen



"Die Ransomware ist so gut [...] Um ehrlich zu sein, oft empfehlen wir Leuten, das Lösegeld einfach zu bezahlen.", erklärte ein Ermittlungsleiter des FBI gegenüber einem Fachpublikum.

 heise Security 27. Oktober 2015, 14:02 Uhr  470

Erpressungstrojaner: Wer Pech hat, zahlt zweimal



Ein Krankenhaus in den USA zahlte das Lösegeld, das Ransomware-Erpresser verlangten. Die Erpresser forderten prompt eine Nachzahlung.

 heise Security 27. Mai, 11:37 Uhr  111

Erpressungs-Trojaner Ranscam schickt Daten unwiederbringlich ins digitale Nirwana



Wie jede Ransomware behauptet auch Ranscam, alle als Geiseln genommenen persönlichen Daten nach einer Lösegeldzahlung freizugeben. In diesem Fall haben das die Drahtzieher aber grundsätzlich gar nicht vorgesehen, warnen Sicherheitsforscher.

 heise Security 12. Juli, 17:11 Uhr  87

FBI: Erpressungstrojaner bringen Millionen ein



Die Welle der Trojaner, die Daten ihrer Opfer verschlüsseln und nur gegen Lösegeld freigeben, ebbt nicht ab. Laut FBI gehen allein die gezahlten Lösegelder für den Trojaner Cryptowall und seine Varianten in die Millionen.

25. Juni 2015, 12:24 Uhr  48

Safer Internet Day: BSI rät Opfern von Ransomware, Anzeige zu erstatten



Wer sich einen Erpressungs-Trojaner eingefangen hat, soll auf keinen Fall das Lösegeld zahlen, rät das BSI. Stattdessen soll man den Bildschirm abfotografieren und Anzeige erstatten.

 heise Security 08. Februar, 15:50 Uhr  63

Statt Backups: Britische Firmen horten Bitcoins für Erpressungstrojaner



Anstatt für regelmäßige Backups zu sorgen, scheinen viele britische Firmen lieber Kryptogeldreserven anzulegen, um Lösegeld für ihre Daten bezahlen zu können. Laut einer Befragung sind viele Firmen bereit, bis zu 50.000 Pfund zu zahlen.

 heise Security 13. Juni, 14:02 Uhr  179

Erpressungstrojaner: FBI hofft auf mehr Anzeigen



Die Erpresser, die Computer kapern und verschlüsseln, werden immer professioneller. In den USA wünscht sich das FBI möglichst viele Anzeigen der Opfer, da jede Information im Kampf gegen die Verbrecher helfen könne.

08. September, 07:19 Uhr  39

Eskalation?

Erpressungs-Trojaner Locky schlägt offenbar koordiniert zu



Locky lauerte vermutlich bereits eine Weile auf den infizierten Systemen, ehe es am vergangenen Montag gleichzeitig bei mehreren Opfern mit der Verschlüsselung persönlicher Dateien begonnen hat.

 heise Security 16. Februar, 15:05 Uhr 653

Erpressungs-Trojaner mit neuer Taktik: Erst schauen, dann verschlüsseln



Nach einem Einbruch in ein Netz verschaffen sich die Erpresser hinter Samsa zunächst Zugriff auf so viele Systeme wie möglich. Erst dann kommt die Verschlüsselung zum Einsatz – und die Opfer bekommen gesalzene Lösegeld-Forderungen.

 heise Security 30. März, 06:30 Uhr 322

Nur 72 Stunden: Erpressungs-Trojaner Jigsaw droht, Dateien zu löschen



Um seine Opfer unter Druck zu setzen das Lösegeld zu zahlen, soll der Verschlüsselungs-Trojaner Jigsaw ständig Dateien löschen, bis die Forderung beglichen ist. Glücklicherweise gibt es bereits ein kostenloses Entschlüsselungs-Tool.

 heise Security 13. April, 14:27 Uhr 157

Erpressungs-Trojaner Locky nun mit Autopilot



Sicherheitsforschern zufolge kann Locky sein Schadenswerk jetzt auch offline ohne Kontakt zum Command-and-Control-Server der Kriminellen verrichten.

 heise Security 15. September, 16:01 Uhr 70

Erpressungs-Trojaner Cerber lernt dazu und verschlüsselt noch mehr



Sicherheitsforscher warnen vor einer neuen Version der Ransomware, die nun unter anderem auch bestimmte laufende Prozesse beenden kann, um so Datenbanken in ihre Fänge zu bekommen.

 heise Security 06. Oktober, 13:44 Uhr 68

Eskalation: Office Makros + PowerShell = Evil

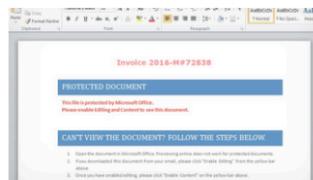
Gefährliches Duo: Erpressungstrojaner kommt mit Word-Datei



Derzeit sollte man jeden Dateianhang in einer E-Mail kritisch betrachten. Denn in letzter Zeit häufen sich Vorfälle, bei denen etwa präparierte Word-Dateien Computer infizieren. Die aktuelle Viren-Welle ist bis ins NRW-Innenministerium vorgedrungen.

 heise Security 10. Dezember 2015, 17:22 Uhr  601

Neue Infektions-Masche: Erpressungs-Trojaner missbraucht Windows PowerShell



Die neu entdeckte Ransomware PowerWare bemächtigt sich der Windows PowerShell, um Computer zu infizieren und Daten zu verschlüsseln.

 heise Security 26. März, 17:57 Uhr  446

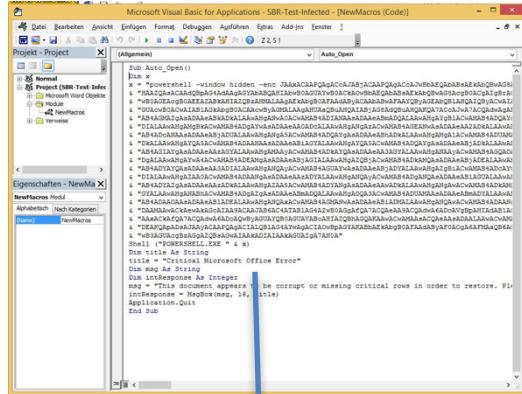
Makroviren – Hacking like it's 1999

- Melissa 1999 aufgetaucht
- Melissa hat sich an alle Kontakte im Adressbuch versendet
- Makroviren eigentlich durch Security Funktionen von Office zwischenzeitlich nahezu ausgestorben
- Seit 2-3 Jahren wieder sehr beliebte
- 2016 Massenhaft für Ransomware genutzt



A black background with green text forming a grid pattern. The text consists of various symbols such as '\$', 'u', and '*' arranged in a repeating pattern. In the bottom right corner, the text 'PRESS ANY KEY!' is displayed in green, followed by four '\$' symbols.

Office Makros + PowerShell - Was passiert?

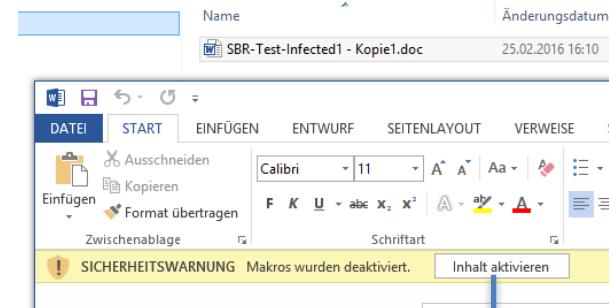


```

Sub Auto_Open()
    Dim title As String
    title = "Critical Microsoft Office Error"
    Dim intResponse As Integer
    intResponse = MsgBox("The document cannot be corrupt or missing critical rows in order to restore. Please, click OK to continue.", 16, title)
    If Application.Quit = True Then
        End
    End Sub

```

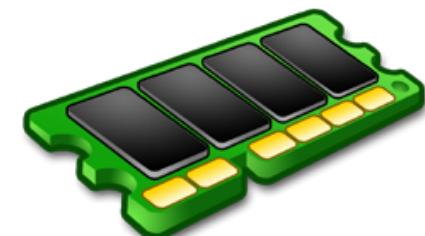
AV



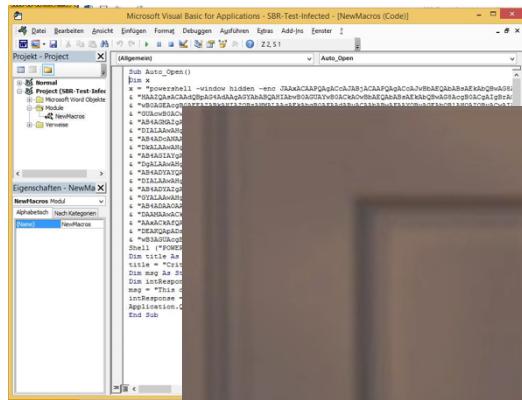
PowerShell
Download



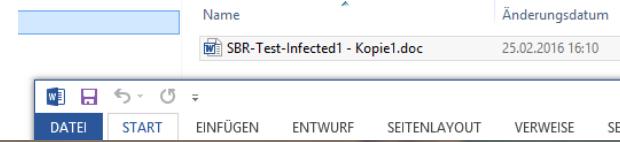
No AV ☹



Office Makros + PowerShell - Was passiert?



```
Sub Auto_Open()
    Dim x As Object
    Set x = New PowerShell
    x.AddScript "window hidden -enc JAxaxC3A9QaACoJ7a8jACAAQgkCoA7vBnAFj2a8s3FxlaBwAd5
    x.Run(")
    x.AddScript "Add-Type -TypeDefinition $x->Get-Content | Out-File C:\Windows\Temp\infected.ps1"
    x.Run(")
    x.AddScript "powershell -ExecutionPolicy Bypass -File C:\Windows\Temp\infected.ps1"
    x.Run(")
End Sub
```



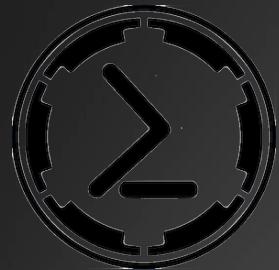
AV



memegenerator.net



Meet PowerShell Empire

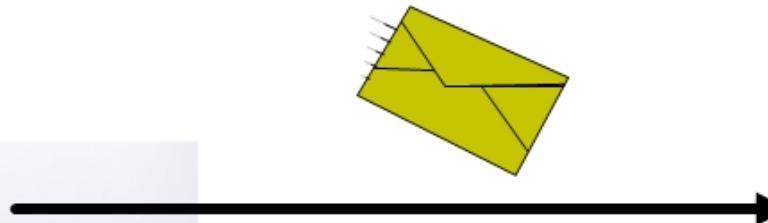


Livedemo!



What could possibly go wrong?

Wait what did just happen?



Präparierte Mail mit gefälschter
Zalando Rechnung



2-Wege-Kommunikation
(Backdoor)



The image shows a YouTube video thumbnail. The title of the video is "Introduction to Empire - Post Exploitation Framework - Offensive Powershell". Below the title, it says "Empire - Develop by @harmj0y, @sixdub and @enigma0x3". The video has a duration of 0:01 / 13:44. The channel name is "HackMeNot" and the subscriber count is 2.901. The video has 6.492 Aufrufe (views). The YouTube interface includes standard controls like play, volume, and share, along with a search bar at the top.

Suchen

Introduction
to
Empire - Post
Exploitation
Framework -
Offensive Powershell

Empire - Develop by @harmj0y,
@sixdub and @enigma0x3

0:01 / 13:44

HackMeNot Jamborloi Calampong

Abonnieren 2.901

6.492 Aufrufe

Hinzufügen Teilen Mehr

53 1

Einiger Lösungsratschlag Heute:

Backups!!!

Sowohl privat auf separater USB HDD!

Als auch im Geschäftlichen Umfeld auf dedizierten
Backup Servern auf die kein normaler User zugreifen
kann!



Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

Sebastian Brabetz
Teamleiter PSS
Telefon 0 55 61/922-397
s.brabetz@it-mod.de

mod IT GmbH
Grimsehlstraße 23
37574 Einbeck
© 2016 mod IT GmbH. Alle Rechte vorbehalten.