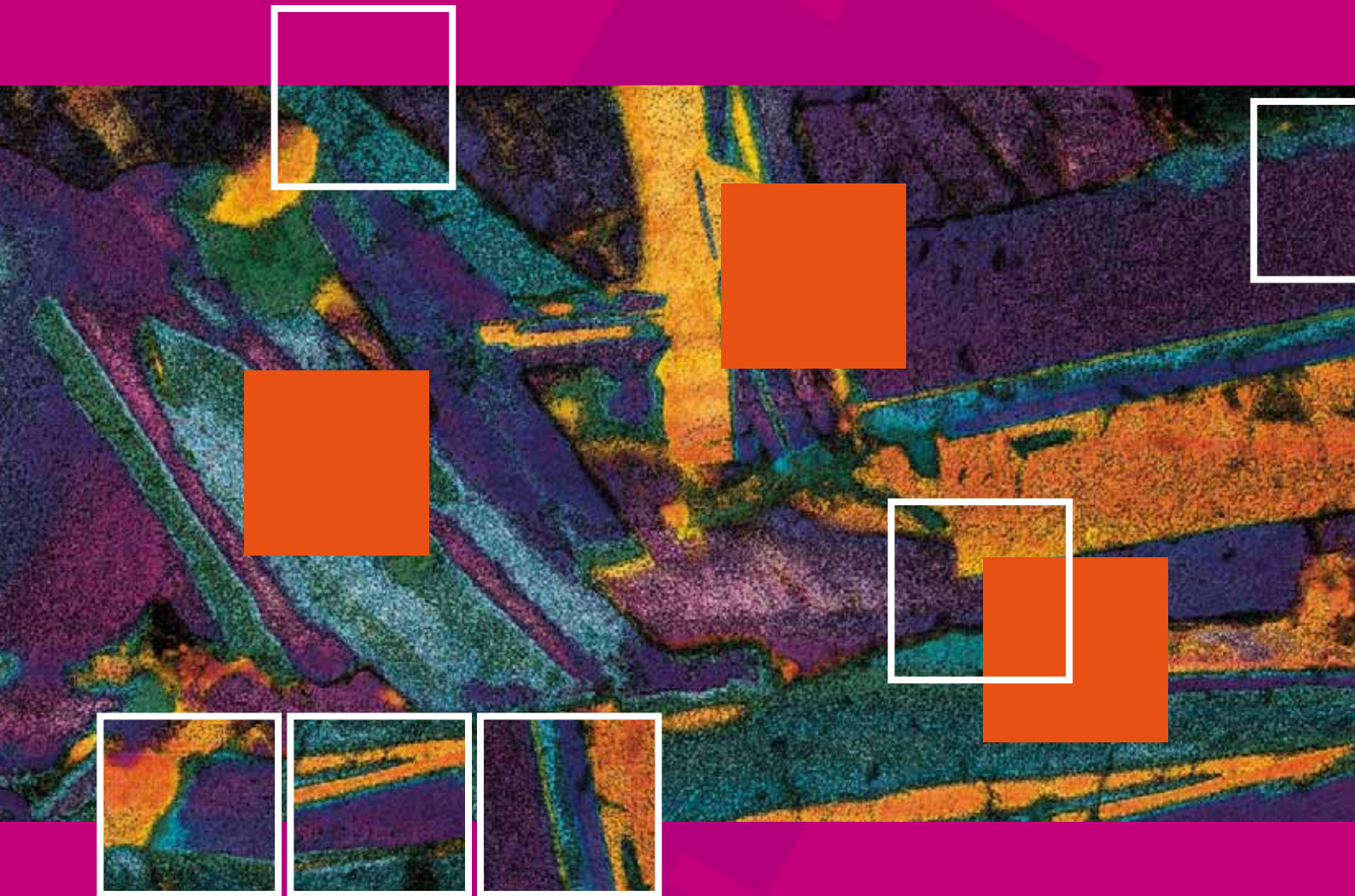


IT SECURITY

2 0 0 7



Unternehmensweite IT-Sicherheit

Konferenz: 18. bis 19.4.2007 – München



Referenten



Joachim Ayasse,
Sicherheitsexperte
GeNUA GmbH



Guntram Geiger,
Geschäftsführer,
GEIGER Maximizing
Net-Solutions GmbH



Dr. Klaus Gheri,
Chief Technology Officer,
phion Technologies AG



Thomas Kerbl,
SEC Consult
Unternehmensberatung
GmbH



Roger Klöse,
Security-Experte,
ERNW GmbH



Thomas Konermann,
Senior Consultant,
TÜV Rheinland
Secure IT GmbH



Lothar Michel,
Geschäftsführer,
Qualys GmbH



Dipl.-Inf. Holger
Morgenstern, öffentlich
bestellter und vereidigter
EDV-Sachverständiger
für Computer Forensik

Die Themen im Überblick

Trotz Viren-, Spam und Spyware-Programmen: Trojaner ante portas

Der Vortrag beleuchtet, wie Trojaner trotzdem immer wieder Rechner auch in Großunternehmen infiltrieren, wie sie funktionieren, welche Mechanismen sie benutzen und wie sie sich verstecken. Live wird ein Trojaner vorgeführt, um die Inhalte des Vortrags konkret vor Augen zu führen.

Sichere Entwicklung von Webanwendungen: Standards und Policies

Es ist unumgänglich, bereits bei der Entwicklung von Webapplikationen hohe Anforderungen an die Codequalität zu legen. Vor allem der Standard ISO 21827 für sichere Softwareentwicklung und die Norm ONR 17700 - Technische Anforderungen für die Sicherheit von Webapplikationen bilden einen ausgezeichneten Rahmen für sichere Entwicklung von Webanwendungen. Im Vortrag werden auch von Policies vorgestellt, die für die nachhaltige Umsetzung von sicherer Software-Entwicklung verwendet werden können.

Sicherheit sensibler Daten: Digital Rights Management

Einige Unternehmen haben damit begonnen, sich gegen die Gefahr von Datenverlusten und Missbrauch von vertraulichen Informationen Digital Rights Management (DRM) Produkte anzusehen. Wir zeigen alternative Techniken, die die Bewegungen von Dateien im Netzwerk und auf jedem betroffenen Endgerät kontrollieren. Dazu werden Agenten auf den Endgeräten oder Sensoren im Netzwerk verwendet. In diesem Vortrag werden die verschiedenen Ansätze sowie ihre Vor- und Nachteile vorgestellt.

Automatisiertes Schwachstellen- und Patch-Management

Ein Ansatz ist, dies Problem mit sogenannten „Scan Engines“, die über das Internet auf Grund einer ständig aktualisierten Liste möglicher Schwachstellen gezielte Schwachstellentests gegen ihre IT-Landschaft durchführen zu lösen. Das es sich um das Modell eines „Software as a Service“ handelt, wird pro IP-Adresse abgerechnet, was sogar im Vergleich zu Open Source-Produkte günstig ist.

Sicheres Netzwerk-Management

Workshopziel: Die Teilnehmer lernen, wie typische Aufgaben im Rahmen des Netzwerk-Managements sicher gestaltet werden können. Es werden Sicherheits-Probleme und Gegenmaßnahmen diskutiert und bewertet. Viele praktische Demos und Beispiele aus komplexen Umgebungen gewährleisten einen hohen Praxis-Bezug.

Integriertes Identity Management und Auditing: Der Schlüssel zur IT-Compliance

Im Workshop werden die Verfahren und Alternativen beschrieben, wie gesetzliche und interne Reglementierungen in operative Regelwerke für die Berechtigungsstrukturen in IT-Systemen übersetzt werden können. Die so genannten preventive controls verhindern im Rahmen der Provisionierung, dass nicht-regelkonforme Berechtigungen erteilt werden. Zusätzlich können systemübergreifend detective controls unzulässige IT-Zugänge aufdecken. Im Rahmen einer Live-Demonstration werden dabei auch die Mechanismen vorgestellt, mit denen die „Heilung“ von Regelverletzungen erfolgen kann.

Digitale Autopsie – Computer-Forensik im Unternehmensalltag

Bei Sicherheitsvorfällen ist es vorteilhaft, wenn der Bereich der Computer-Forensik vorausschauend in den gesamten Incident-Response-Prozess integriert wird. Das Auffinden und Analysieren digitaler Spuren muss so geschehen, dass diese später in einem Gerichtsverfahren verwendet werden können. Unterstützt wird dieser Prozess durch moderne Computer-Forensik Werkzeuge sowohl aus dem kommerziellen wie auch aus dem Open-Source Bereich.

SAP-Netweaver Portal: Live Hacking

Anhand eines fiktiven SAP-Systems zeigen wir live, wie Angreifer Schwachstellen und Passwörter ermitteln können. Dies kann im schlimmsten Fall sogar den Zugriff auf die zentrale Datenbank des Unternehmens ermöglichen. In Step 2 werden von uns die Sicherheitsrisiken und ihre möglichen Auswirkungen dargestellt. Schließlich werden die Erkenntnisse in eine Schutzbedarfs- und Risikoanalyse umgesetzt und geeignete Maßnahmen zur Reduktion der Risiken aufgezeigt.

Segen oder Fluch? Cisco Network Admission Control

Aggressiv vermarktet Cisco das „Self-Defending-Network“, dessen Kernkomponente das „Network Admission Control“ bildet. Diese Technologie soll garantieren, dass nur Clients, die einer definierten Policy entsprechen, Zugang zum Netz erhalten. Nach einem Blick auf die



Funktionsweise der Technologie werden Schwachstellen in der NAC-Architektur aufgezeigt und Ansätze zum sicheren Betrieb einer NAC-Lösung diskutiert.

Data Center: Gesichertes Netzwerkdesign

Im IT-Bereich steigen die Sicherheitsanforderungen an Rechenzentren, Server- und Back-up-Räume kontinuierlich. Eine IT-gerechte, maßgeschneiderte passive Netzwerkinfrastruktur bedeutet ein gesichertes Netzwerkdesign, das Anwendern ein höchstes Maß an Funktionalität, Übersichtlichkeit und die daraus resultierende Sicherheit und Verfügbarkeit über die Norm hinaus garantiert.

Checklisten zur MPLS-Sicherheit

MPLS ist die mittlerweile wichtigste Backbone-Technologie grosser Netze und wird inzwischen in vielen Organisationen nicht nur als Produkt zur VPN-Realisierung eingekauft, sondern zur logischen Verkehrstrennung auch zunehmend in Campus-Netzen eingesetzt. Übersehen wird dabei häufig, dass MPLS sich hinsichtlich möglicher Sicherheitsprobleme oder Angriffs-Szenarien von seinen „Vorgängern“ Frame-Relay oder ATM deutlich unterscheidet. Der Vortrag thematisiert Sicherheits-Aspekte beim Einsatz von MPLS und darauf basierender Dienste. Es wird zudem auch eine Checkliste vorgestellt, mit der MPLS-Sicherheit bewertet werden kann.

Routing-Security 2007: Stand der Technik

Die geroutete Infrastruktur bildet das Rückgrat unserer Netzwerke. Dabei vernachlässigen viele Unternehmen die Sicherheit der Routing-Infrastruktur. Erfolgreiche Angriffe auf Routingprotokolle ermöglichen die Unterwanderung vieler darauf aufbauender Sicherheitsmechanismen. Neben praktischen Angriffen auf Routingprotokolle werden verfügbare Sicherheitsmechanismen und ihre Wirksamkeit erläutert.

Risikomanagement: Beyond the line – Information Security Risk Management

Im Rahmen der Implementation eines ISMS wird immer auch die Implementation eines Risikomanagements gefordert. Dieses bildet die Grundlage für alle weiteren Aspekte des ISMS und ergänzt das bestehende Risikomanagement einer Organisation um die Aspekte des operativen Risikos im Umgang mit Informationen. Dabei treten bei der Implementation eines Risikomanagements unterschiedliche Probleme auf, die für einen nachhaltigen und sinnvollen Betrieb eines ISMS nach 27001 gelöst werden müssen.

Corporate Security: Reporting System

Security Management-Systeme müssen in der Lage sein, unternehmensweit alle Anwender mit vielfältigen Aufgabenstellungen und Rollen in die Sicherheitsmanagement-Prozesse einzubinden und optimal zu unterstützen. Durch eine effiziente Informationsverarbeitung und offene Schnittstellen können sie sich optimal in die unternehmensspezifische IT-Welt integrieren. Ein Modul mit Business-Logik und Regelwerk gewährleistet die Konformität zu anerkannten Risikomanagement und Sicherheitsmanagement-Normen, internen Richtlinien und einzuhaltenden Gesetzen.

SOA und die richtige IT Security-Antwort

Die umfassende Sicherung einer SOA gegen Angriffe ist eine große Herausforderung, da SOA ein neues Sicherheitsmodell erfordert, in dem viele altbewährte Lösungen für Benutzermanagement, Authentifizierung, Autorisierung, Föderation usw. nicht mehr funktionieren. Dieser Vortrag zeigt die spezifischen Sicherheitsprobleme von SOA aus der Architektur- und Managementperspektive und bietet Lösungsstrategien an. Ausgehend von der Architektur, über Integration von Sicherheitskonzepten in die Entwicklung, die korrekte Auswahl der Komponenten und einer klaren Einordnung der vielen WS-* Spezifikationen, wird eine ganzheitliche Sicht auf die Sicherheit von SOA angeboten. Konkrete Angriffsszenarien werden besprochen, so dass die Methoden der Hacker (und daher die Schwächen der SOA) ersichtlich werden.

Security Management: Prozesse-Technologien-Lösungsansätze

Gefragt sind innovative Lösungsansätze für dieses Problem, indem gleichzeitig die drei wesentlichen Kundenanforderungen adressiert werden: Verfügbarkeit, Sicherheit und zentrales Management. Unternehmenskritische Dienste wie Firewall, VPN, Mail-Gateway oder auch http-Proxy und DNS-Services werden zu einer einheitlichen Infrastruktur verbunden, die über zentrale Management-Server verwaltet werden kann. Damit werden die Leistungsfähigkeit eines Unternehmensnetzwerks gesteigert und gleichzeitig die Gesamtkosten (TCO) drastisch gesenkt.

Service-orientierte Security

Unternehmen beginnen zunehmend die IT-Infrastruktur service-orientiert zu betrachten. Dies gilt selbstverständlich auch für die IT-Sicherheit. Es geht nicht darum, das komplette Unternehmen unter Security-Aspekten zu betrachten, sondern sich auf die relevanten Services zu konzentrieren.

Referenten



Ulrich Parthier,
Publisher IT SECURITY



Marcel Read,
Geschäftsführer,
comratio GmbH



Dror-John Röcher,
CISSP, Senior IT
Security Consultant,
ERNW GmbH



Dr. Bruce Sams,
Geschäftsführer
optima bit GmbH



Stefan Strobel,
Geschäftsführer,
cirosec GmbH



Eckhard Völcker,
Vorstand
Völcker Informatik AG



Dr. Oliver Weissmann,
Teamleiter
Strategie-Sicherheit,
help AG



Dominik Witte,
SecureIntegration GmbH



18. April 2007

08:30 – 09:00 **Registrierung & Second Breakfast**

Block 1: Internet Security

09:00 – 09:45 **Trotz Viren-, Spam und Spyware-Programmen: Trojaner ante portas**

Joachim Ayasse, Sicherheitsexperte, GeNUA GmbH

- Die Gefahr lauert überall
- Das Danaergeschenk
- Versteckte Soldaten
- Die Stadt fällt

09:45 – 10:30 **Sichere Entwicklung von Webanwendungen: Standards und Policies**

Thomas Kerbl, SEC Consult Unternehmensberatung GmbH

- Webapplikationen als schwächstes Glied
- ISO 21827 als Standard für sichere Softwareentwicklung
- ONR 17700 als Standard für sichere Webapplikationen
- Policies für die nachhaltige Umsetzung sicherer Software-Entwicklung

10:30 – 11:00 **Kommunikationspause**

BLOCK 2: Security Management

11:00 – 11:45 **Sicherheit sensibler Daten: Digital Rights Management**

Stefan Strobel, Geschäftsführer, cirosec GmbH

- Bedrohungen für sensible Daten im Unternehmen
- Verschiedene Lösungsansätze
- Vor- und Nachteile der vorgestellten Lösungsansätze
- Handlungsempfehlungen

11:45 – 12:30 **Automatisiertes Schwachstellen- und Patch-Management**

Lothar Michel, Geschäftsführer, Qualys GmbH

- Nutzen von Vulnerability-Scanns
- Automatisierung durch Scan Engines
- Reporting mit Hilfe eines web-basierten Workflows
- Kostenkontrolle dank IP-Kostenmodell

12:30 – 13:30 **Business Lunch**





18. April 2007

BLOCK 3: Workshops (bitte zwischen A - B - C wählen)

13:30 – 15:00

A: Sicheres Netzwerk-Management*Roger Klose, Security-Experte, ERNW GmbH*

- SNMPv3: Architektur & Konfiguration
- Device-Zugriff: SSH vs. Telnet, Arbeit mit Jump Hosts, das Problem Web-Interfaces
- Sichere Konfigurations- und Image-Verwaltung, Integritätsprüfung von Konfigs,
- Logging & Log-Auswertung: Protokolle & Formate

B: Integriertes Identity Management und Auditing: Der Schlüssel zur IT-Compliance*Eckhard Völcker, Vorstand Völcker Informatik AG*

- Rechtliche und technische Rahmenbedingungen
- Systemübergreifendes Management von IT-Berechtigungen
- Preventive und detective controls zur Verhinderung und Aufdeckung von Regelverstößen
- Live-Demo

C: Digitale Autopsie – Computer-Forensik im Unternehmensalltag*Dipl.-Inf. Holger Morgenstern, EDV-Sachverständiger für Computer-Forensik*

- Sicherheitsvorfälle, gezielte Angriffe und Spionage im Alltag
- Integration der Computer-Forensik in den Incident-Response-Prozess
- Digitale Spuren finden und gerichtsverwertbar sichern
- Aktuelle Computer-Forensik Werkzeuge im Vergleich

15:00 – 15:30

Kommunikationspause

BLOCK 4: SAP-Sicherheit – Live Szenarien

15:30 – 16:15

SAP NetWeaver Portal: Live Hacking*Dominik Witte, SecureIntegration GmbH*

- Vorstellung des Systems
- Identifizierung der Angriffspunkte
- Schutzbedarf- und Risikoanalyse
- Umsetzung von Schutzmaßnahmen

16:15 – 17:00

Segen oder Fluch? Cisco Network Admission Control*Dror-John Röcher, CISSP, Senior IT Security Consultant, ERNW GmbH*

- Wunschdenken der Marketiers
- Die Wirklichkeit
- Funktionsweise der Technologie
- Vorschläge für den sicheren Betrieb

17:00 – 17:30

Closing Session: Data Center – Gesichertes Netzwerkdesign*Guntram Geiger, Geschäftsführer, GEIGER Maximizing Net-Solutions GmbH*

- Schwachstellen
- Strukturen
- Dokumentation
- Normen

Ab 19:00

Festliches Dinner (Casual Dress) – Kubanischer Abend!



19. April 2007

BLOCK 5: Netzwerksicherheit

09:00 – 09:45 **Checklisten zur MPLS-Sicherheit**
Roger Klose, Security-Experte, ERNW GmbH

- Kauf ohne Sicherheitscheck
- Unterschiede zu Frame Relay und ATM
- Einsatzmöglichkeiten und daraus resultierende Lücken
- Checkliste zur Sicherheit von MPLS

09:45 – 10:30 **Routing-Security 2007: Stand der Technik**
Dror-John Röcher, CISSP, Senior IT Security Consultant ERNW GmbH

- Status in den Unternehmen
- Sicherheitslücken
- Angriffe (Live)
- Sicherheitsmechanismen

10:30 – 11:00 **Kommunikationspause**

BLOCK 6: Risk Management & Reporting

11:00 – 11:45 **Risikomanagement: Beyond the line – Information Security Risk Management ISO 27005**
Dr. Oliver Weissmann, Teamleiter Strategie-Sicherheit, help AG

- Umgang mit Komplexität – Identifikation von Assets/Unternehmenswerten
- Vernetzung von Abhängigkeiten
- Beurteilung von Risikofaktoren
- Darstellung von Risiken

11:45 – 12:30 **Corporate Security Reporting System**
Marcel Read, Geschäftsführer, comratio GmbH

- Anforderungen an ein Corporate Security Reporting-System
- Kritische Erfolgsfaktoren bei der Auswahl und Inbetriebnahme
- Workflow-Design, IT und organisatorische Aspekte der Management-Prozesse
- Toolunterstütztes Reporting und Praxiserfahrungen

12:30 – 13:30 **Business Lunch**

BLOCK 7: Workshops (bitte zwischen A - B - C wählen)

13:30 – 15:00 **A: SOA und die richtige IT Security-Antwort**
Dr. Bruce Sams, Geschäftsführer optima bit GmbH

- Sicherheitsmodelle
- Architektur und Managementsicht
- Lösungsstrategien
- Konkrete Angriffsszenarien



19. April 2007

B: Security Management: Prozesse-Technologien-Lösungsansätze

Dr Klaus Gheri, CTO, phion Technologies AG

- Komplexität von IT-Infrastrukturen
- Spannungsfeld Verfügbarkeit, Sicherheit und zentrales Management
- Innovative Lösungsansätze
- Umsetzungsbeispiele

C: CSO Cockpit: Toolunterstütztes Security Information Management

- Compliance Check
- Proaktives Risikomanagement
- Visuelle Security Information Map
- Überwachung nach dem CACA-Modell

15:00 – 15:30 **Kommunikationspause**

BLOCK 8: Security Management – Live Szenarien

15:30 – 16:15 **Service-orientierte Security**

Thomas Konermann, Senior Consultant, TÜV Rheinland Secure IT GmbH

- Grundlagen Security-Prozesse nach ISO 27001
- Service-orientierte Betrachtung
- Vorgehensmodell
- Praxisbeispiel anhand eines eMail-Push-Dienstes

16:15 – 17:00 **Interne Sicherheit: Die nächste Generation**

- Methoden interner Netzwerk-Angriffe und Abwehrstrategien
- Praxis- und Anwenderbeispiele: WLAN und VoIP Internal Security
- Innovative und wirtschaftliche Lösungskonzepte
- Handlungsstrategien

17:00 – 17:30 **Abschluss des 2. Tages und Heimreise**





Anmeldung

Faxantwort + 49 8104 649422

Veranstaltungsort:
Holiday Inn München-Unterhaching
Inselkammerstraße 7-9
82008 Unterhaching
S-Bahnstation Unterhaching (S5)

Name

Firma

Funktion

Straße

PLZ/Ort

Tel.-Nr.

Fax-Nr.

E-Mail

Teilnahmebedingungen

- Hiermit melde ich mich verbindlich zur Konferenz „Unternehmensweite IT-Sicherheit“ in München an.
- Frühbucherrabatt bis 16. März 2007 740.– Euro zzgl. MwSt. inklusive Apple iPod nano 4 Gbyte.
bitte ankreuzen: schwarz weiß pink grün blau
- Ab dem 17. März 2007 840.– Euro zzgl. MwSt.



Alle Preise verstehen sich zzgl. der zum Zeitpunkt der Rechnungsstellung gesetzlichen MwSt.

Rechnungsanschrift (falls abweichend)

Es gelten die AGBs des IT Verlag für Informationstechnik GmbH. Diese sind mir bekannt und jederzeit unter www.it-verlag.de einsehbar.

Datum

Stempel/rechtsverbindliche Unterschrift