T.I.S.P. Community Meeting

Berlin, 14. - 15.11.2017

Next-Generation Endpoint Security

Von Marketing-Blasen und vielversprechenden Technologien

Lars Koch, DCSO GmbH

Deutsche Cyber-Sicherheitsorganisation GmbH

Allianz · BASF We create chemistry · BAYER · VOLKSWAGEN AKTIENGESELLSCHAFT

Community Information Services	Cyber Defense Services	Professional Services
Technology Scouting & Evaluation	Threat Intelligence	Governance, Risk & Compliance
Audit	Information Leakage Monitoring	Technical Consulting
Cloud Vendor Assessment	Threat Detection & Hunting	Integration Engineering
	Incident Response	

Think Tank Research & Development Projects

DCSO ENGINEERING SECURITY

DCSO ENGINEERING SECURITY

Keine Sorge, der Perimeter schützt uns!

Ja, aber wie gut?

Endpoint im Fokus

- Angriffstechniken
  - Social Engineering
    - Spear Phishing
  - Drive-by-Downloads
  - Hardware-basierende Attacken (z.B. USB)
  - Oft mehrere Angriffsschritte und Lateral Movement
  - Insider Threat

The Initial Compromise

The Initial Compromise represents the methods intruders use to first penetrate a target organization's network. As with most other APT groups, spear phishing is APT1's most commonly used technique. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file.

Die häufigsten Infektionswege für Schadprogramme sind E-Mail-Anhänge sowie die vom Anwender unbemerkte Infektion beim Besuch von Webseiten, sogenannte Drive-by-Downloads.

COMPUTER USERS PASS around USB sticks like silicon business cards. Although we know they often carry malware

Quellen: Mandiant – APT 1, BSI – Die Lage der IT-Sicherheit in Deutschland 2017

Endpoint im Fokus

- Technische Herausforderungen
  - Ende-zu-Ende Verschlüsselung
    - S/MIME, PGP
    - Verschlüsselte Anhänge
    - HTTP Public Key Pinning (HPKP)
  - Remote Arbeitsplatz / Home Office
    - VPN Bypass?
  - Sales Team auf Reise

APT intruders most commonly use the RAR archiving utility for this task and ensure that the archives are password protected.

Quelle: Mandiant – APT 1

DCSO ENGINEERING SECURITY

Was ist Endpoint Security im klassischen Sinne?

Endpoint Security – was wir bisher darunter verstanden haben

- Prinzip: **Prevention & Protection**

- Anti-virus Software auf Workstations
  - Regelmäßige Signatur-Updates
- Host Firewall, VPN Connector
- Festplattenverschlüsselung
- Application Control
- Device Control

DCSO ENGINEERING SECURITY

Und was ist dann Next-Generation Endpoint Security?

NGES – was sagen die Hersteller?

*[…] Next Generation Platform to provide the broadest **enterprise visibility** and accurate detection of advanced threats & evasion techniques, and **zero-day attacks** by utilizing behavioral analytics, machine learning, and Long-Data Security-Analytics.*

*By coupling sophisticated math and **machine learning** with a unique understanding of a hacker's mentality, […] provides the technology and services to be truly predictive and preventive against advanced threats*

*[…] prevents **advanced attacks** and zero-days when and where they happen – at your endpoints and in real time, with **zero false positives** and no performance degradation.*

Bitte… was?!

DCSO ENGINEERING SECURITY

Wir müssen uns an neue Vokabeln gewöhnen

Buzzword Bingo, Anyone?

Lightweight Agent	EDR	Ransomware	Signature-less	Next-Gen
Lateral Movement	Machine Learning	Defense in Depth	Remediation	Zero-Day Protection
Cloud-based	Threat Hunting	Indicator of Compromise	Kill Chain	Sandboxing
Threat Intelligence	Offline Protection	Zero False-Positives	Remote Task Execution	RESTful API
Real-time	Exploitation Mitigation	Advanced Persistent Threat	Network Containment	Behavior Analysis

NGES – Wichtige Features

Lightweight Agent	EDR	Ransomware	**Signature-less**	Next-Gen
Lateral Movement	Machine Learning	Defense in Depth	**Remediation**	Zero-Day Protection
Cloud-based	Threat Hunting	**Indicator of Compromise**	Kill Chain	Sandboxing
Threat Intelligence	**Offline Protection**	Zero False-Positives	**Remote Task Execution**	**RESTful API**
Real-time	**Exploitation Mitigation**	Advanced Persistent Threat	**Network Containment**	**Behavior Analysis**

DCSO ENGINEERING SECURITY

Wenden wir sie doch mal an…

NGES – Beispiel

Provides intelligent EDR with automated real-time detections
Ensures continuous monitoring and visibility
Accelerates investigation and remediation with full context detections and alerts

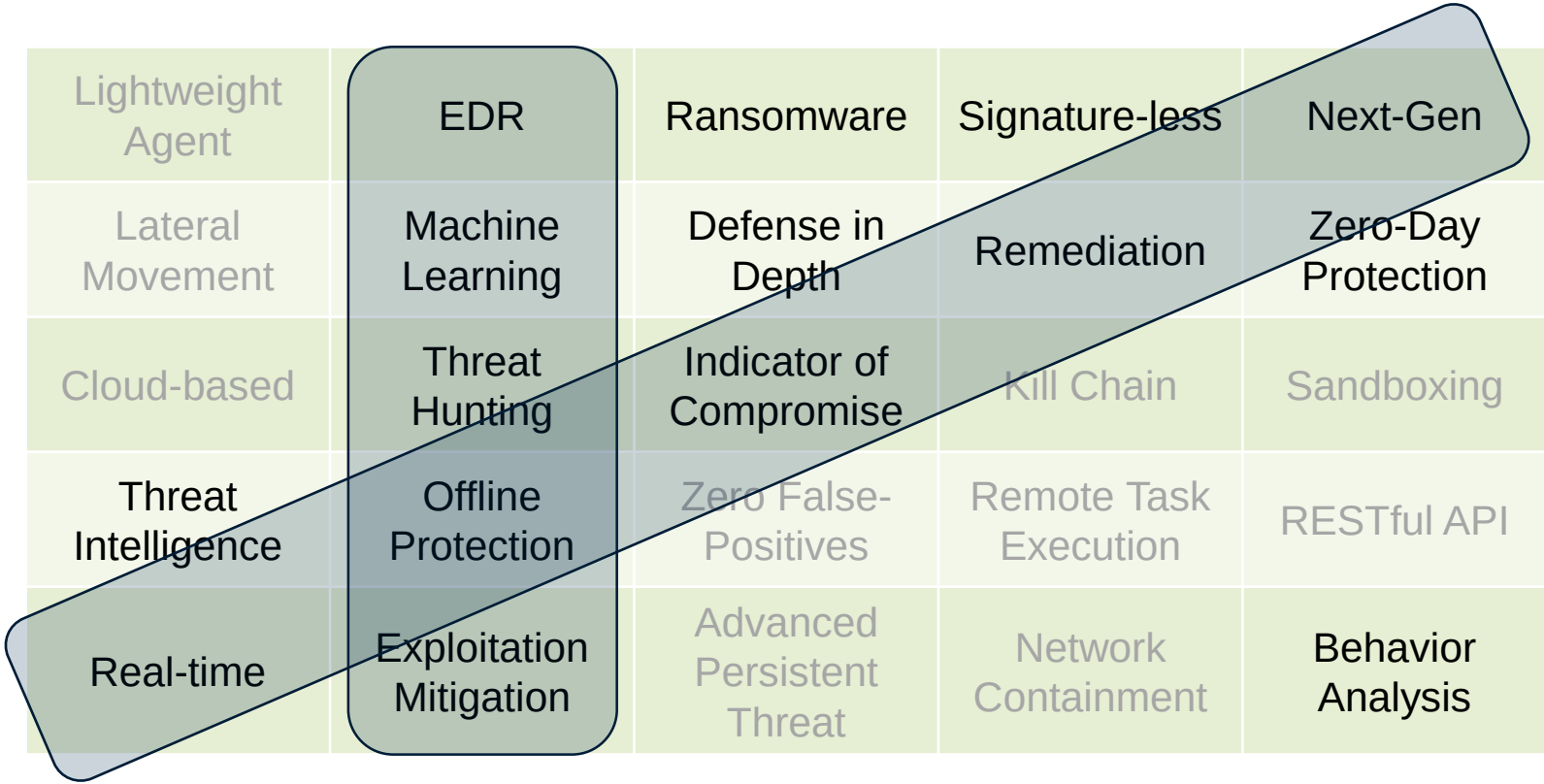
Obtain attack attribution
Gain insight on who might be targeting you and how to defend against them
Maximize your defenses with in-depth, actionable security analysis and reporting

Protects your endpoints against all threat types – known and unknown, malware and malware-free
Combines machine learning malware protection, Indicator of Attack (IOA) behavioral blocking and exploit blocking for ultimate protection
Eliminates ransomware
Requires no signature updates
Delivers full protection even when offline

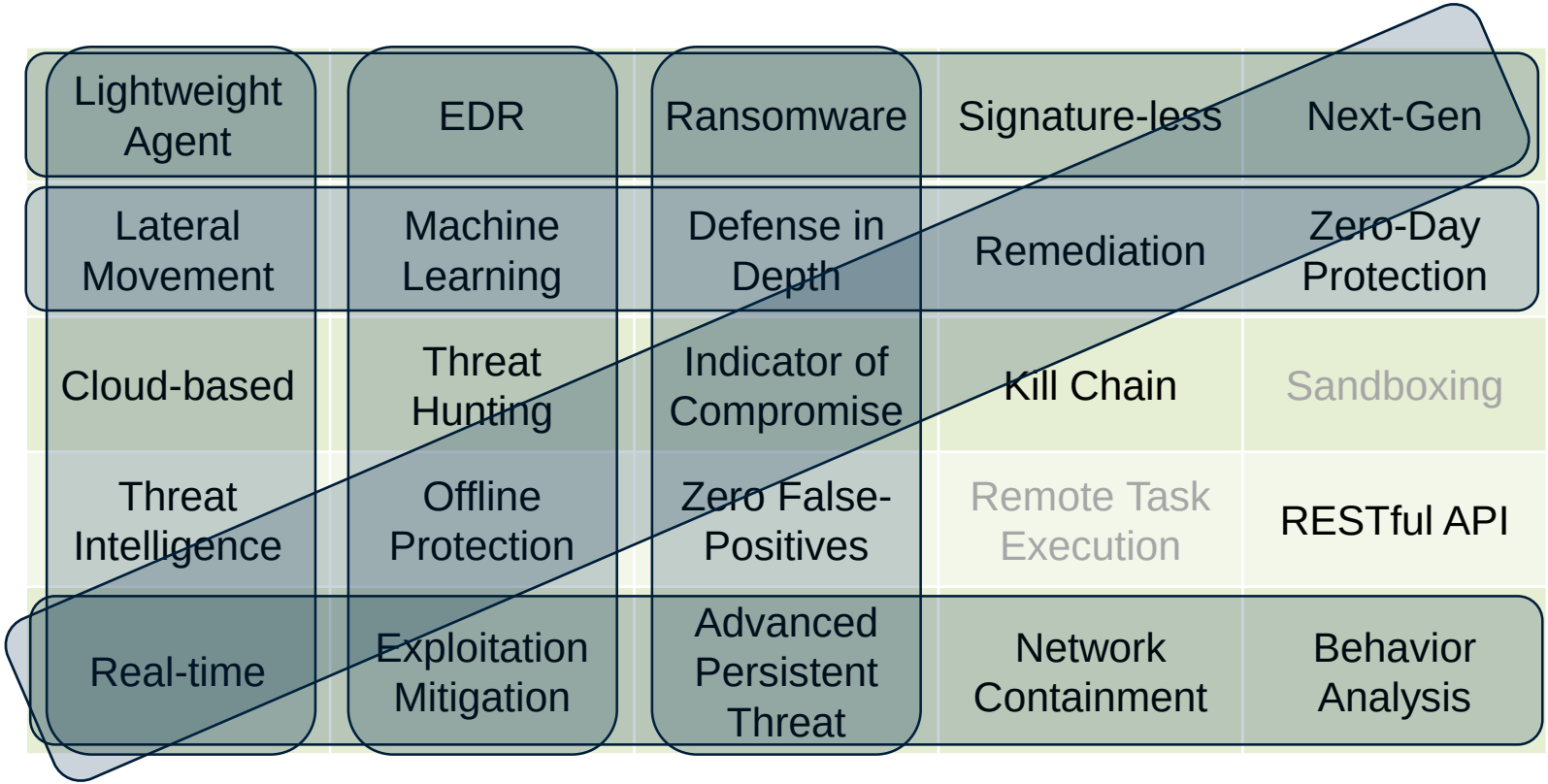
[redacted] endpoint protection unifies the technologies required to successfully stop breaches: next-generation antivirus, endpoint detection and response, IT hygiene, 24/7 threat hunting and threat intelligence. They combine to provide continuous [redacted]

Fully operational in seconds
No reboot required
No performance impact on endpoints
No need for AV signature updates
No need for fine-tuning or configuration
No need for additional infrastructure

Zwei Treffer – ein guter Start



Sieben Treffer – geht doch



DCSO ENGINEERING SECURITY

Welche Ansätze und Strategien gibt es aktuell?

NGES – neue Ansätze und Strategien

Endpoint Prevention & Protection (EPP)

- IoC-basierende Malware Erkennung
- Statische Analyse
- Memory Exploitation Mitigation
- Verhaltensanalyse
- *Machine Learning*
- Virtualisierung & Isolation von Anwendungen
- Exploitation Mitigation
- Automatische System-wiederherstellung (Remediation)

Endpoint Detection & Response (EDR)

- Datensammlung & Event Korrelation
- IoC-basierende Malware Erkennung
- Beweissicherung
- Fernzugriff auf Endpoint
- *Machine Learning*

Bestreben, EDR-Funktionalität zu implementieren

Bestreben, EPP-Funktionalität zu implementieren

Einige Technologien im Detail

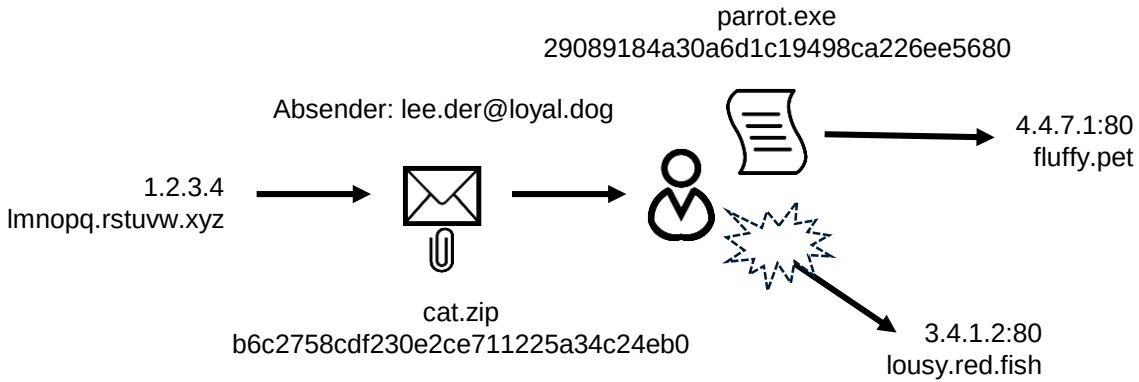
EPP & EDR – Signaturen und IoC-basierende Malware Erkennung

- NGES Hersteller reagieren allergisch auf Signaturen!
  - Hashes bekannter Dateien
  - Malware Erstellung schneller als Signatur Updates
  - Signaturen dennoch sinnvoll

- Indicator of Compromise
  - Logische Verknüpfung beobachtbarer Events (+ Kontext)
  - Threat Intelligence Feeds
    - CybOX (Wörterbuch für Cyber Observable)
    - STIX (XML-Schema, das CybOX Wörter strukturiert)
    - TAXII (bestimmt, wie STIX ausgetauscht wird)

EPP & EDR – Signaturen und IoC-basierende Malware Erkennung

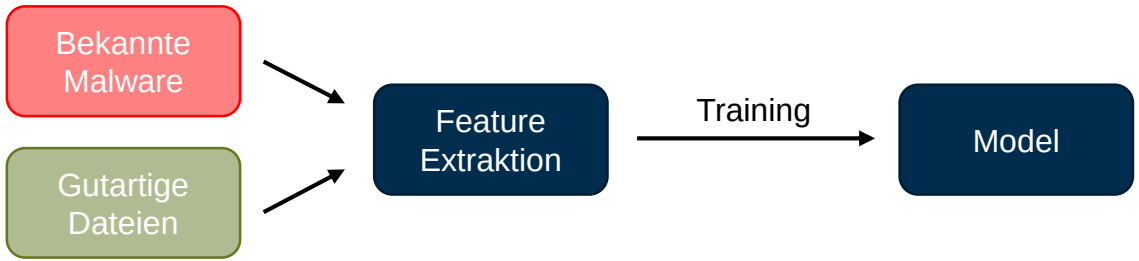
- Indikatoren (Beispiel)
  - Aufruf der URL http://lousy.red.fish
  - Maileingang von 1.2.3.4 mit Absender lee.der@loyal.dog und Anhang cat.zip
  - Prozess parrot.exe ruft URL http://fluffy.pet/ auf



EPP – Statische Analyse von Binaries

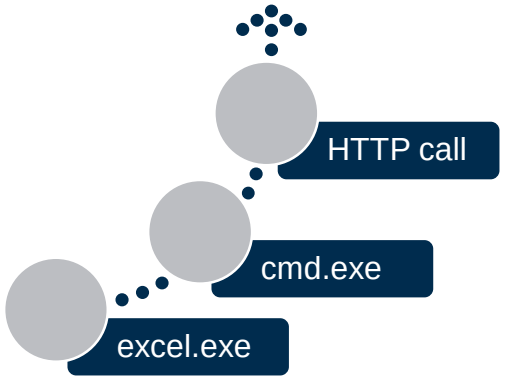
- Überprüfung der binären Merkmale von Dateien (insb. Executables)
  - Imports und Exports von Symbolen
  - Compiler
- Obfuscation
  - Verschleierung der Programmlogik
  - Genaues Laufzeitverhalten unklar

- Machine Learning



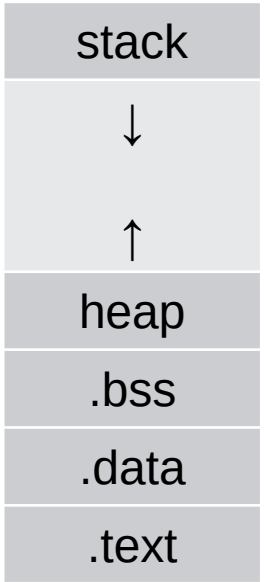
EPP – Verhaltensanalyse

- Beobachtung von Prozessverhalten
  - Oft durch IoC beschrieben
  - Ungewöhnliche Prozessaktivitäten?
    - System Calls
    - Subprozesse
  - Ungewöhnliches Kommunikationsverhalten?
- Eingebettete Skripte
  - Microsoft Office Macros, VBA, PowerShell, …



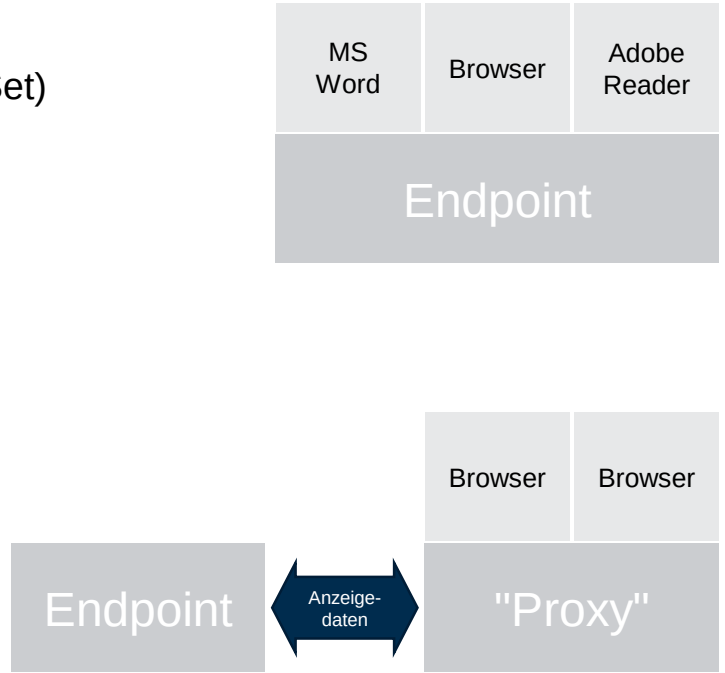
EPP – Memory Exploitation Mitigation

- Schutz des (Prozess-)speichers vor Manipulation
  - Durch Verwürfelung des Speicherlayouts (ASLR)
  - Durch Absichern von Exception Handlern (SEHOP)
  - Durch Verhindern von Code-Ausführung aus bestimmten Speicherbereichen (DEP)
  - Beschränken von Symbol-Imports (IAF, EAF)
- Kernel Space
- Achtung vor Inkompatibilitäten



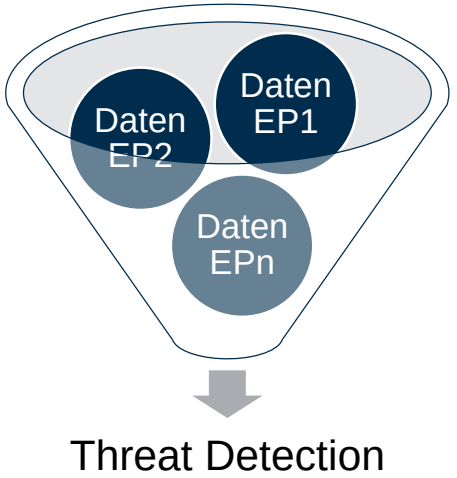
EPP – Virtualisierung und Isolation von Anwendungen

- Virtualisierungsschicht auf dem Endpoint
  - Mit Hardware-Unterstützung (VT-x CPU Feature Set)
- Anwendung wird in separater VM gestartet
  - Begrenzte Anwendungsunterstützung
  - Potente Hardware notwendig
  - Exploits wirken nur in VM
- Automatischer Rollback bei Beenden
  - Verarbeitete Dateien über Filter gespeichert
- Teilweise Verhaltensanalyse innerhalb VM
- Browservirtualisierung auf zentralem "Proxy"



EDR – Datensammlung & Event Korrelation

- Zentrale Sammlung von Endpoint Daten
  - Benutzer & Systemaktivitäten
  - Gestartete Prozesse
  - Netzwerkverbindungen
  - Dateizugriffe
- Identifikation ungewollter Aktionen
  - Machine Learning
- Teilweise Korrelation zwischen Endpoints
  - Identifikation von Lateral Movement
- Ransomware Identifikation
  - Ressourcen-intensiver Prozess
  - Viele kryptographische Operationen
  - Viele Dateizugriffe in kurzer Zeit



Erkenntnisse aus halben Jahr Umgang mit NGES Produkten

NGES – Unsere Erkenntnisse

- NGES umfasst viele unterschiedliche Ansätze
- Kein Produkt deckt aktuell alle NGES Fähigkeiten komplett ab

- Erkennung von Malware blieb hinter den Erwartungen zurück
- Überraschend geringer Automatisierungsgrad, oft manuelle Aktionen notwendig

- Unterschiedliche Architekturen, oft Cloud Backend
- "Enterprise Readiness" meist nur stiefmütterlich implementiert
- Integrationsfähigkeit zunehmend wichtiger (und oft stark ausgeprägt)

- Traditionelle Hersteller "leben" noch

Worauf Sie bei der Auswahl eines NGES Produktes achten sollten

- Werden Fähigkeiten aus EPP und EDR unterstützt?
  - Welche strategische Entwicklung strebt der Hersteller an?
  - Wie klar werden eingesetzte Technologien beschrieben? (Machine Learning ≠ Machine Learning)
- Sind klassische Funktionen enthalten?
  - Application Control
  - Device Control
- Wie *Enterprise Ready* ist das Produkt?
  - Product Life Cycle
  - HA Fähigkeit, Backup & Restore
  - Intuitives Policy Management
  - Integrationsfähigkeit (AD, SIEM, SEOA,…)

Spielen Sie NGES Bingo!

Lars Koch
Security Analyst
DCSO GmbH
Mob: +49 151 43157839
E-Mail: lars.koch@dcso.de

DCSO Deutsche Cyber-Sicherheitsorganisation GmbH
Rosenthaler Straße 40 (Hackesche Höfe)
10178 Berlin