

# Incident Response


---

aus polizeilicher Sicht



# Agenda

---

- Vorstellung
  - Reale Fallbeispiele
  - Rolle der Polizei
  - Aktuelle Studie
  - Incident Response Maßnahmen
    - Datensicherungen
    - Auswertung
  - Fazit
- 

# Vorstellung

---

- Andreas Dondera
- aka Donde
- 25 Jahre Polizeibeamter
- 8 Jahre Lehre und Administration
- reiner Autodidakt
- IT-Ermittler und Forensiker
- Anregungen geben, sich mit dem Thema „IT-Forensik“ zu beschäftigen

# Reale Fallbeispiele

- Aktuelle Beispiele für Cybercrimedelikte in Firmen:
  - Kompromittierung von Netzwerken durch aktive / ehemalige Mitarbeiter / Admins
  - Ausspähen von Daten in Firmennetzwerken (aktuell z.B. Reedereien)
  - Manipulierte E-Mails im geschäftlichen Zahlungsverkehr
  - DDOS-Angriffe mit/ohne Erpressungshintergrund
  - Gezieltes Ausspähen von Daten bei hochrangigen Mitarbeitern
  - „Klassisches Hacking“ (z.B. SQL-Injection)
  - TK-Anlagen Hacking (Phreaking)
- Beispiele für Cybercrimedelikte bei Privatpersonen
  - verschiedenste Betrugsdelikte (Ebay, Fakeshops, Finanzagenten, usw.)
  - Phishing / Malware:
    - Ausspähen von Accounts
    - Übernahme von Rechnern
  - Urheberrecht → hat in Hamburg praktisch keine Bedeutung im Strafrecht!!!

# Polizei

- Zuständigkeiten bei Cybercrime-Delikten
  - Polizei ist Ländersache
  - Zuständigkeit ist Delikts- und Ortsabhängig
  - BKA-Zuständigkeit nur in sehr vereinzelt Fällen
  - LfV hat in Hamburg keine Ermittlungsbefugnisse
- Polizeiliche Rahmenbedingungen (Hamburg)
  - Technische Ausstattung ist gut
  - Personelle Ausstattung wird besser ;-)
  - Fachwissen stark verbesserungswürdig
  - keine Informatiker im Bereich der Ermittlungen

# Strafverfahren

- Herrin des Verfahrens ist die Staatsanwaltschaft
- Strafanzeige ist an keine Form gebunden
- Cybercrime sind fast sämtlich Antragsdelikte -> Strafantrag erforderlich (Antragsberechtigter?)
- Die Polizei ist die Behörde die von der StA mit der Ermittlung des Täters beauftragt wird
- Polizei übermittelt die Akte nach Abschluss der Ermittlungen zur Beschlussanregung an die StA
- StA entscheidet nach Aktenlage über die Einstellung des Verfahrens, Strafbefehl, Anklageerhebung oder weitere Ermittlungen

# Ablauf einer Strafanzeige

- schriftliche Anzeige direkt an die Staatsanwaltschaft (StA):
  - Briefkasten → Poststelle StA → zuständige StA-Abteilung → Zuschreibung Staatsanwalt → zuständige Polizeidienststelle → Poststelle StA → Poststelle Polizei → Polizeidienststelle → Zuschreibung Sachbearbeiter
  - Zeit bis zur Aufnahme der Ermittlungen ca. 5-7 Tage (in Hamburg)
- Anzeigenerstattung an einer Polizeiwache:
  - Anzeigenaufnahme → Poststelle Polizei → Polizeidienststelle → Zuschreibung Sachbearbeiter
  - Zeit bis zur Aufnahme der Ermittlungen ca. 2 Tage (in Hamburg)
- Anzeige per Fax an zuvor kontaktierte Dienststelle
  - Faxeingang → Zuschreibung Sachbearbeiter
  - Zeit bis zur Aufnahme der Ermittlungen i.d.Regel unter einer Stunde

# Polizeiliche Probleme

---

- Speicherfristen
  - IP-Adressen können selten zugeordnet werden
  - Mobilfunkbereich noch schwieriger
- Antwortzeiten von IT-Dienstleistern
- Offene Rechtsfragen
- Internationalität
- Anonymisierung / Kryptographie
- Elektronischer Geldfluss
- Technische Veränderungen (z.B. IPv6)
- aber auch: keine kompetenten Ansprechpartner



# Studie aus dem Jahr 2013

---

- ~7500 Unternehmen aus verschiedenen Branchen wurden zu IT-Sicherheitsvorfällen befragt
- ~33% der Unternehmen gaben an, dass in den letzten 12 Monaten ihre IT-Infrastruktur angegriffen wurde
- nur ~13% zeigten den Vorfall bei der Polizei an!
- Gründe keine Anzeige zu erstatten:
  1. Aufwand der Anzeigenerstattung zu groß
  2. Keine Erfolgsaussichten
  3. Kein Ansprechpartner vorhanden
  4. Angst vor Reputationsverlust
  5. Mögliche Störungen des Produktivbetriebs

# Stellungnahme zu den Gründen

---

## 1. Aufwand der Anzeigenerstattung zu groß?

- wie bereits ausgeführt reicht ein Fax.

## 2. Keine Erfolgsaussichten?

- Kommt auf den Fall an.  
Bei Innentäter → oftmals recht gute Erfolgschancen

## 3. Kein Ansprechpartner vorhanden?

- VOR einem Sicherheitsvorfall Ansprechpartner ermitteln

## 4. Angst vor Reputationsverlust

- Umgang mit der Polizei im Unternehmen klären
- Bistlang im LKA Hamburg keine „Verluste“ dieser Art bekannt


## 5. Sorge vor Störungen des Produktivbetriebs

- ggf. auf eigene Ermittlungen und Datensicherungen vorbereiten

Vorteil: Unterstützung bei der Aufklärung des Vorfalls

# Ursachen für Angriffserfolge

---

- mangelndes Problembewusstsein
  - schlechte Wartung der Systeme
  - „gewachsene“ Systeme
  - schlechte / keine Dokumentation
  - mehrere IT-Dienstleister
  - Admin- Mitarbeiterwechsel
  - unzureichende Fachkenntnisse
- 

# Incident Response

Sicherheitsvorfall ist eingetreten

Zwei Möglichkeiten:

1. Polizei wird eingeschaltet, erscheint kurzfristig vor Ort und ist in der Lage die Beweissicherung zeitnah und fachgerecht durchzuführen.
2. Die Polizei kann nicht (zeitnah) erscheinen oder soll nicht eingeschaltet werden
  - Folge:
    - (mehr) eigene Maßnahmen erforderlich
    - gerichtsfeste Datensicherung (z.B. zivilrechtl. Ansprüche)
    - (forensische) Analyse des Vorfalls

# Sicherungsmaßnahmen

---

- Art und Umfang hängen vom Einzelfall ab
- ALLE Maßnahmen DOKUMENTIEREN!
  - Flüchtige Daten sichern
  - Netzwerktraffic dumpen
  - Datenträger sichern
  - Datensicherungen je nach Vorfall analysieren, z.B.
    - Logfiles auswerten
    - komplette Systeme auswerten
    - Zeitlinienanalyse
    - Malwareuntersuchung
    - usw.

# Flüchtige Daten

- Die Sicherung flüchtiger Daten verändert das System!
  - Schritte daher gut dokumentieren
  - keine System-Binaries verwenden
  - Einstecken von USB-Sticks zieht bereits Änderungen nach sich (z.B. Laden von Kernelmodulen)
  - ggf. über das Netzwerk sichern (z.B. netcat)
- relevante Informationen (Auswahl):
  - Prozesslisten
  - Netzwerkverbindungen
  - Offene Dateien
  - aktive User
- es existieren zahlreiche Skripte, die dieses durchführen

# RAM sichern

- Linux:
  - Download von lime
  - kompilieren des lime-Moduls
  - `sudo insmod lime.ko "path=/ram.dd format=lime"`
- Nachteil:
  - C-Compiler + Kernel-Header auf Produktivsystem
- Alternativ
  - Kernelmodul auf externem System erstellen und aktuell halten
  - Kosten / Nutzen Abwägung
- VMware: VM pausieren (Ramdump in MASCHINENNAME.vmem)
- Windows: Moonsols Tools (`win64dd.exe /r /f ram.dd`)

# RAM analysieren

---

- Tool der Wahl ist Volatility
- Profildatei muss erstellt werden
  - module.dwarf + Sytemmap
- über 40 Linux-Plugins in Volatility z.B.:
  - linux\_ifconfig → aktive Netzwerkinterfaces
  - linux\_lsof → offene Dateien
  - linux\_lsmod → geladene Module
  - linux\_netstat → offene Sockets
  - linux\_psaux → aktive Prozesse
  - usw.



# Netzwerkanalyse

- Verdacht unrechtmäßiger Aktivitäten durch
  - externe Angreifer
  - Mitarbeiter (z.B. Rechteexkalation)
  - Malwareverdacht
- Proxy vorhalten
  - Rechner mit zwei Netzwerkkarten
  - Linux-Distribution
  - mit „bridge-utils“ als transparenten Proxy konfigurieren
  - Proxy vor betroffenem System einhängen
  - Aufzeichnen/Filtern des Datenverkehrs
    - `sudo dumpcap -i ethx -b filesize:100000 -w blafa.pcap`
    - `tshark -r blafa.pcap -R '$Filterregel' -w blafa_filtered.pcap`

# Datensicherung erstellen

- Grundsätzlich immer eine physikalische Datensicherung erstellen
- Schreibschutz für Datenträger gewährleisten (Forensik-Distri o. Hardware)
- Datensicherung immer mit Hashwert überprüfen
- Sicherungsvorgang dokumentieren
  
- Forensikformate:
  - RAW (dd, img) → Sicherungsgröße = Datenträgergröße  
dc3dd if=/dev/sdX of=blafa.dd bufsz=1M log=blafa.log
  - EWF (E01) → Komprimierung, Metadaten, proprietär, teilweise offene Spez.  
ewfacquire -l blafa.log /dev/sdaX
  - AFF → Komprimierung, Metadaten, geringe Verbreitung, offen
  
- Sicherung über Netzwerk
  - Sicherungsverzeichnis per sshfs (fuse) mounten → ewfacquire
  - dc3dd Ausgabe über nc auf Sicherungs-PC pipen

# Datensicherung untersuchen I

---

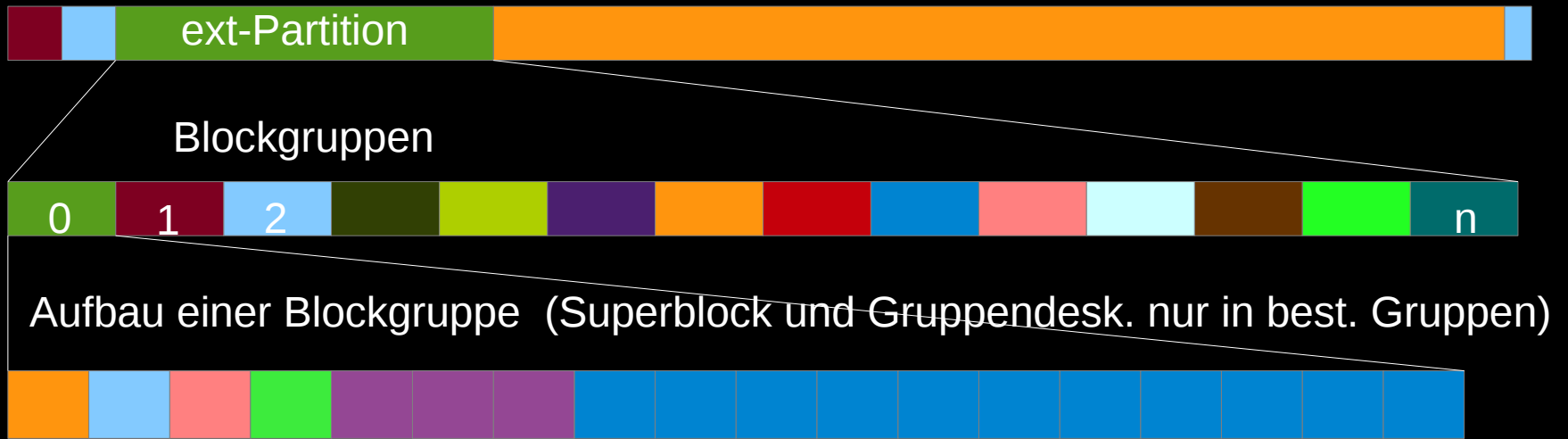
## Dateibasierter Ansatz mit „Sleuthkit“:

- Vorhandene Dateien
- Gelöschte Dateien
  - nur der Dateisystemlink wurde entfernt
  - Datei partiell überschrieben
  - usw.
- File Slack

## Zeitbasierter Ansatz mit „log2timeline“:

- Erstellen einer Zeitlinie über ein oder mehrere Systeme, um zu analysieren, was zu einem Zeitpunkt X passiert ist.
- Zeiten aus Dateizeitstempeln
- Logfiles
- Registry
- usw.

# Dateisystem ext 2/3/4



- Superblock (Anzahl Inodes, Blöcke, Mounts, letzter Mount, usw.)
- Gruppendedeskriptor (Pos. BlockBitmap, InodeBitmap, usw. f. jede Gruppe)
- Blockbitmapblock (Belegungszustand Blöcke)
- Inodebitmapblock (Belegungszustand Inodes)
- Inodebitmactable (128 Byte pro Datei, Rechte, Blockadressen, usw.)
- Datenblöcke

# Slackspace

Datenblock 4096 Byte = 8 Sektoren a -derzeit noch typisch- 512 Byte

geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD
-----------------------------	-----------------------------	-----------------------------	-----------------------------	-----------------------------	-----------------------------	-----------------------------	-----------------------------

Der obige Block gehört zu einer gelöschten Datei „Secrets.txt“

Ein User erstellt eine neue Datei namens „Brief an Oma.txt“.

Die Datei endet in dem zuvor gelöschten, obigen Block.

FOLGE → Slackspace

Essen gut und das Wetter war toll	Alles Liebe Dein Jan	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD	geheim, secret VS NfD
--	-------------------------	-----------------------------	-----------------------------	-----------------------------	-----------------------------	-----------------------------	-----------------------------

RAM Slack

File Slack

# Datensicherung untersuchen II

---

The Sleuth Kit (TSK) von Brian Carrier:

- mm = media management
- fs = filesystem
- i = inode
- f = file
- stat = statusinformationen
- ls = auflisten von Informationen
- cat = entspricht dem normalen cat
- Beispiel:
  - fls = listet Dateien auf
  - icat = erstellt Inhalt anhand eines Inodes

# Zeitlinienanalyse

---

log2timeline (plaso) von Kristinn Gudjonsson:

- Parser für verschiedene Dateitypen
  - Zeitangaben aus Metadaten (EXIF)
  - Zeitangaben aus der Registry
  - Zeitangaben aus Logfiles
  - Zeitangaben aus Dateien (MACB)
  - Zeitangaben aus Browserhistory
  - Zeitangaben aus Recycler
  - usw.

# Malwareuntersuchung

---

- Desinfekt auf die Datensicherung anwenden (benötigte Pakete z.B. xmount nachinstallieren)
- ggf. gefundene Viren in Standalonesystem einbinden:
  - MS Attack Surface Analyser
  - BSA und Sandboxie
- ggf. Datensicherung in Virtualisierung (qemu) starten
  - RAM-Dump erstellen und analysieren
- Malware in Form von PHP-Skripten auf Webservern
  - regelmäßig obfuskiert
  - evalhook von Stefan Esser



# Fazit

---

## Incident Response:

- zu informierende Personen bestimmen
- Umgang mit der Polizei vorab klären
- frühzeitig zuständige Dienststelle ermitteln
- Anzeigenberechtigte benennen
- Sicherheitsvorfall vorbereiten
  - ggf. Vorkehrungen für RAM-Dump (Kernel-Modul)
  - ggf. transparenten Proxy vorhalten
  - Tools für Datensicherung bereithalten
  - Umgang mit den vorgenannten Programmen testen

Ende

---

Fragen?

Kontakt:

[andreas.dondera@polizei.hamburg.de](mailto:andreas.dondera@polizei.hamburg.de)

[lka54@dondera.de](mailto:lka54@dondera.de)

Key-ID: 60C6FC5F