cirosec

# Ganzheitliche Bewertung technischer Maßnahmen für Malwareschutz

# Grundidee

- Gegenüberstellung von Maßnahmen für Malwareschutz und Erkennung gegen die relevanten Bedrohungsszenarien in einer Matrix
  - Inwieweit schützt die jeweilige Technik tatsächlich vor den Bedrohungen, vor denen sie schützen soll?
  - Wie gut können Kompromittierungen erkannt werden?

- Ziel ist es, Maßnahmen vergleichen zu können
  - Welche Maßnahme erkennt / schützt gegen welche Malware-Szenarien?
  - Wo sind die technologie-bedingten Grenzen des Schutzes?
  - Wie ergänzen neue Maßnahmen die bestehende Infrastruktur?

# Stark vereinfachtes Beispiel

cirosec

| | AV-Signaturprüf. | Appl. Whitelisting | Exploit Mitigation | Device Kontrolle | MS-Office-Härtung |
|---|---|---|---|---|---|
| Bösartiges Exe-File per Web-Download  | | | | | |

# Stark vereinfachtes Beispiel

| | AV-Signaturprüf. | Appl. Whitelisting | Exploit Mitigation | Device Kontrolle | MS-Office-Härtung |
|---|---|---|---|---|---|
| Bösartiges Exe-File per Web-Download  | Mittlerer Schutz | Hoher Schutz | Kein Schutz | Kein Schutz | Kein Schutz |

# Stark vereinfachtes Beispiel

| | AV-Signaturprüf. | Appl. Whitelisting | Exploit Mitigation | Device Kontrolle | MS-Office-Härtung |
|---|---|---|---|---|---|
| Bösartiges Exe-File per Web-Download  | Mittlerer Schutz | Hoher Schutz | Kein Schutz | Kein Schutz | Kein Schutz |
| E-Mail mit bösartigem Excel-Makro  | Mittlerer Schutz | Kein Schutz | Kein Schutz | Kein Schutz | Hoher Schutz |

# Stark vereinfachtes Beispiel

| | AV-Signaturprüf. | Appl. Whitelisting | Exploit Mitigation | Device Kontrolle | MS-Office-Härtung |
|---|---|---|---|---|---|
| Bösartiges Exe-File per Web-Download  | Mittlerer Schutz | Hoher Schutz | Kein Schutz | Kein Schutz | Kein Schutz |
| E-Mail mit bösartigem Excel-Makro  | Mittlerer Schutz | Kein Schutz | Kein Schutz | Kein Schutz | Hoher Schutz |
| PDF-Dokument mit Exploit von Website  | Mittlerer Schutz | Kein Schutz | Hoher Schutz | Kein Schutz | Kein Schutz |

# Stark vereinfachtes Beispiel

cirosec

| | AV-Signaturprüf. | Appl. Whitelisting | Exploit Mitigation | Device Kontrolle | MS-Office-Härtung |
|---|---|---|---|---|---|
|  Bösartiges Exe-File per Web-Download | Mittlerer Schutz | Hoher Schutz | Kein Schutz | Kein Schutz | Kein Schutz |
|  E-Mail mit bösartigem Excel-Makro | Mittlerer Schutz | Kein Schutz | Kein Schutz | Kein Schutz | Hoher Schutz |
|  PDF-Dokument mit Exploit von Website | Mittlerer Schutz | Kein Schutz | Hoher Schutz | Kein Schutz | Kein Schutz |
|  Powershell-Malware auf USB-Stick | Mittlerer Schutz | Mittlerer Schutz | Kein Schutz | Hoher Schutz | Kein Schutz |

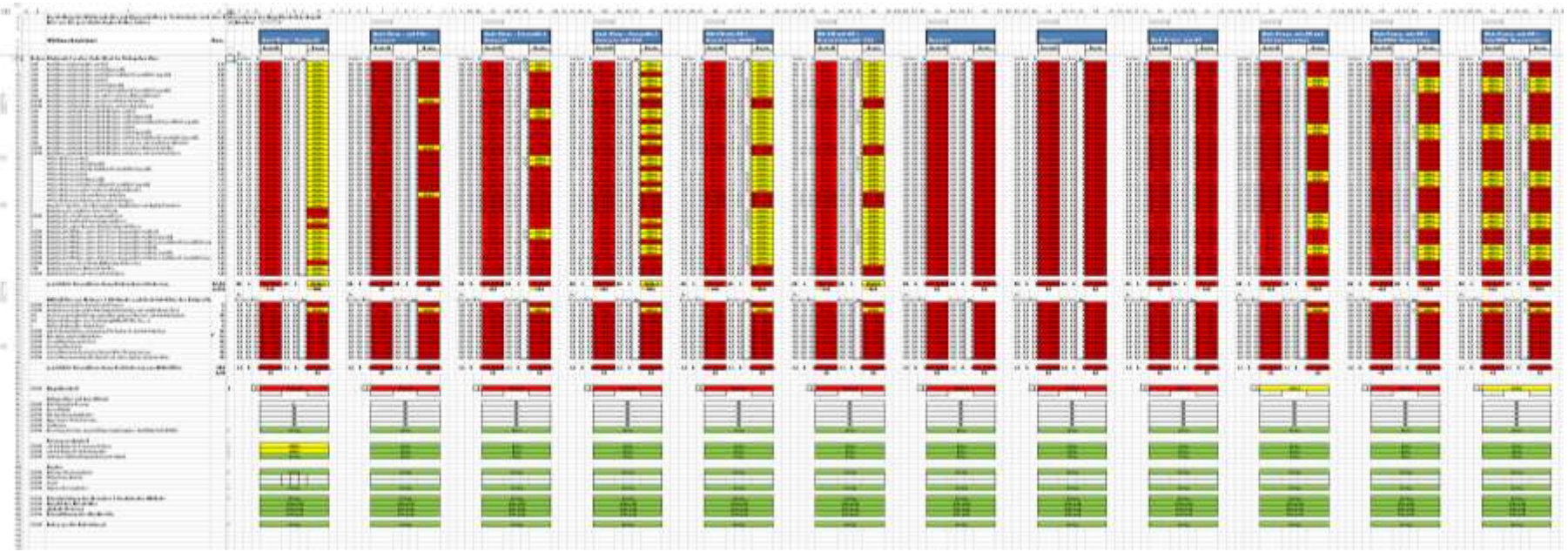
# Stark vereinfachtes Beispiel

cirosec

| | AV-Signaturprüf. | Appl. Whitelisting | Exploit Mitigation | Device Kontrolle | MS-Office-Härtung |
|---|---|---|---|---|---|
|  Bösartiges Exe-File per Web-Download | Mittlerer Schutz | Hoher Schutz | Kein Schutz | Kein Schutz | Kein Schutz |
|  E-Mail mit bösartigem Excel-Makro | Mittlerer Schutz | Kein Schutz | Kein Schutz | Kein Schutz | Hoher Schutz |
|  PDF-Dokument mit Exploit von Website | Mittlerer Schutz | Kein Schutz | Hoher Schutz | Kein Schutz | Kein Schutz |
|  Powershell-Malware auf USB-Stick | Mittlerer Schutz | Mittlerer Schutz | Kein Schutz | Hoher Schutz | Kein Schutz |
|  Ausführbarer Schadcode über Software-Update | Mittlerer Schutz | Kein Schutz | Kein Schutz | Kein Schutz | Kein Schutz |

# Gesamteindruck einer Bewertungsmatrix

cirosec

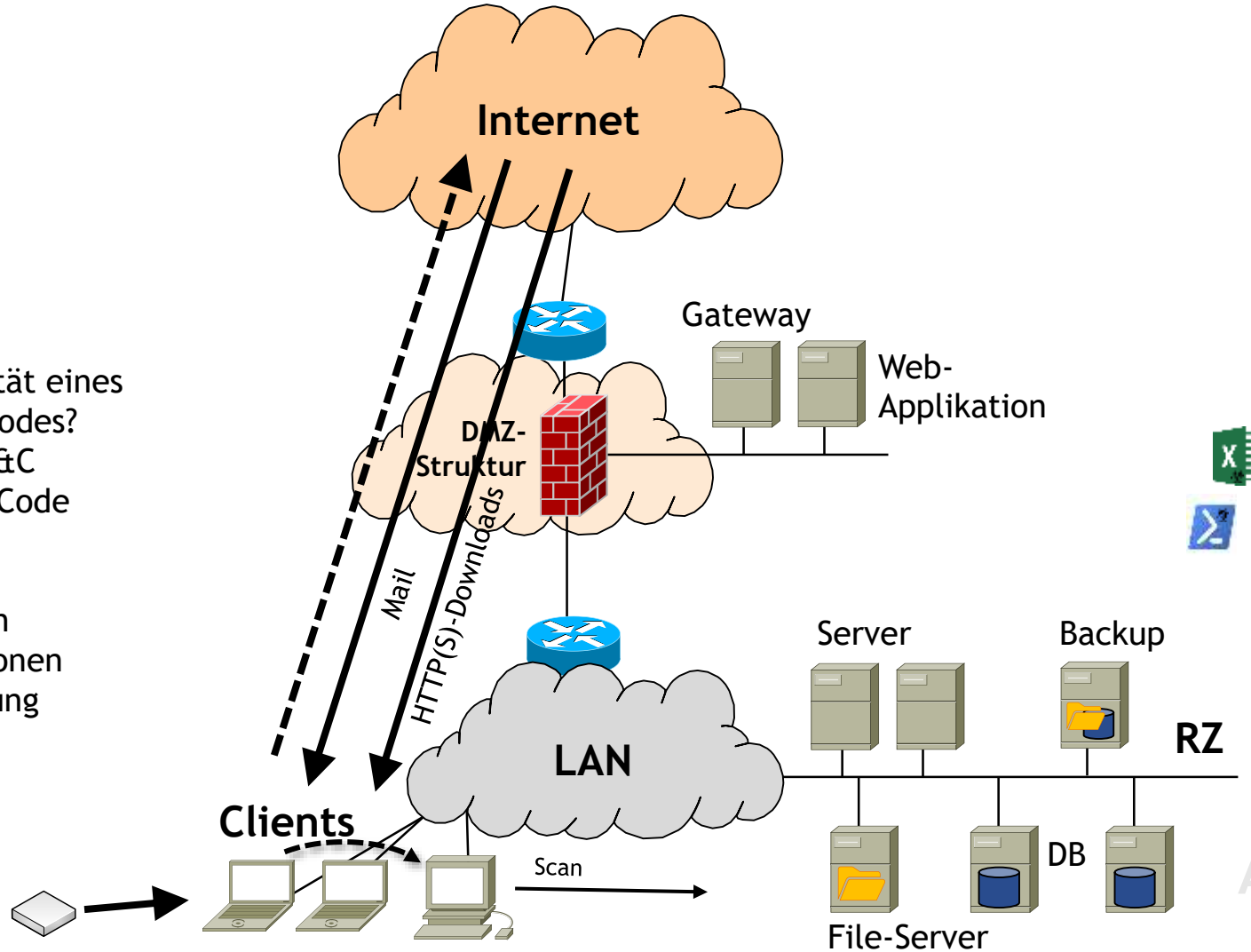


# Aufbau der Matrix:
# Gliederung der Bedrohungsaspekte

cirosec

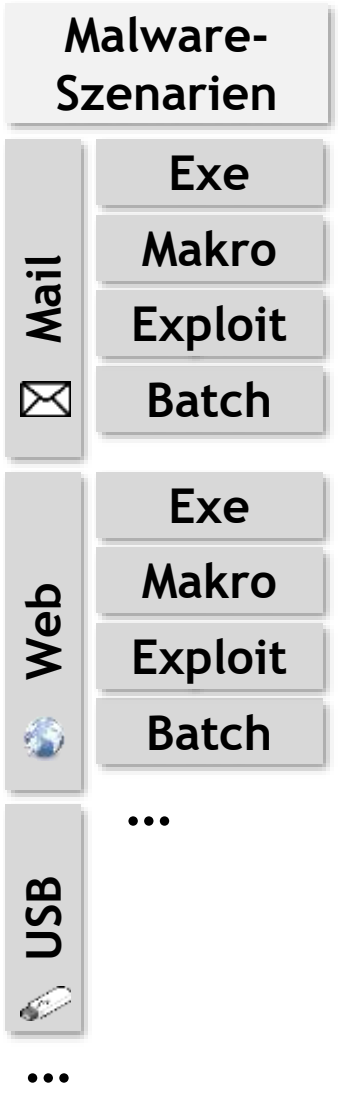
Für welche Infektionswege?
- Mail
- Web
- USB
- VoIP / P2P / …
- SW-Updates
- Erreichbare Dienste

Für welche Aktivität eines laufenden Schadcodes?
- DNS-Tunnel / C&C
- Nachladen von Code
- CMD.exe
- Scanning
- Datenextraktion
- File-Manipulationen
- Registry-Änderung
- …




Für welche Techniken?
- Ausführbares Programm
- BAT / PowerShell-Script
- Office-Makro
- PDF-Exploit
- Flash-Exploit
- …

# Die Vorgehensweise konkreter dargestellt




- Zunächst muss eine vollständige Liste aus den Unterscheidungsachsen für Malware-Szenarien gebildet werden
  - Übertragungsweg
  - Innerhalb jedes möglichen Übertragungs-weges nach Startmechanismus des Schadcodes
  - Verhalten bzw. Schadfunktionen nach der ersten Infektion

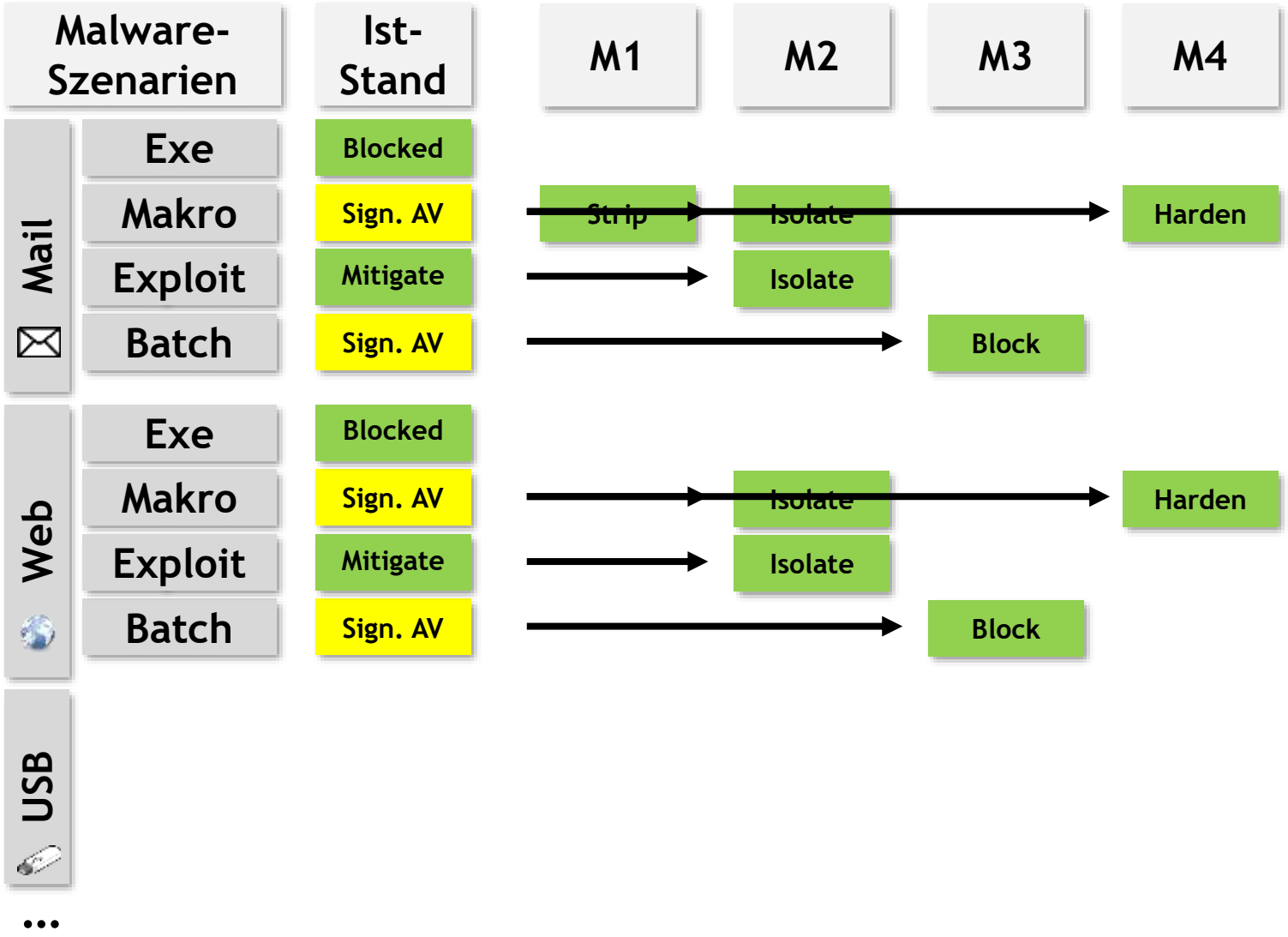
# Erfassen und Bewerten der vorhandenen Maßnahmen

| Malware-Szenarien | | Mail GW | Web Proxy | Exploit Guard | App Locker |
|---|---|---|---|---|---|
| Mail | Exe | Blocked | Kein Schutz | Kein Schutz | Blocked |
| | Makro | Sign. AV | Kein Schutz | Kein Schutz | Kein Schutz |
| | Exploit | Sign. AV | Kein Schutz | Mitigate | Kein Schutz |
| | Batch | Sign. AV | Kein Schutz | Kein Schutz | Kein Schutz |
| Web | Exe | Kein Schutz | Sign. AV | Kein Schutz | Blocked |
| | Makro | Kein Schutz | Sign. AV | Kein Schutz | Kein Schutz |
| | Exploit | Kein Schutz | Sign. AV | Mitigate | Kein Schutz |
| | Batch | Kein Schutz | Sign. AV | Kein Schutz | Kein Schutz |
| ... | | ... | ... | ... | ... |
| USB | | | | | |
| ... | | | | | |

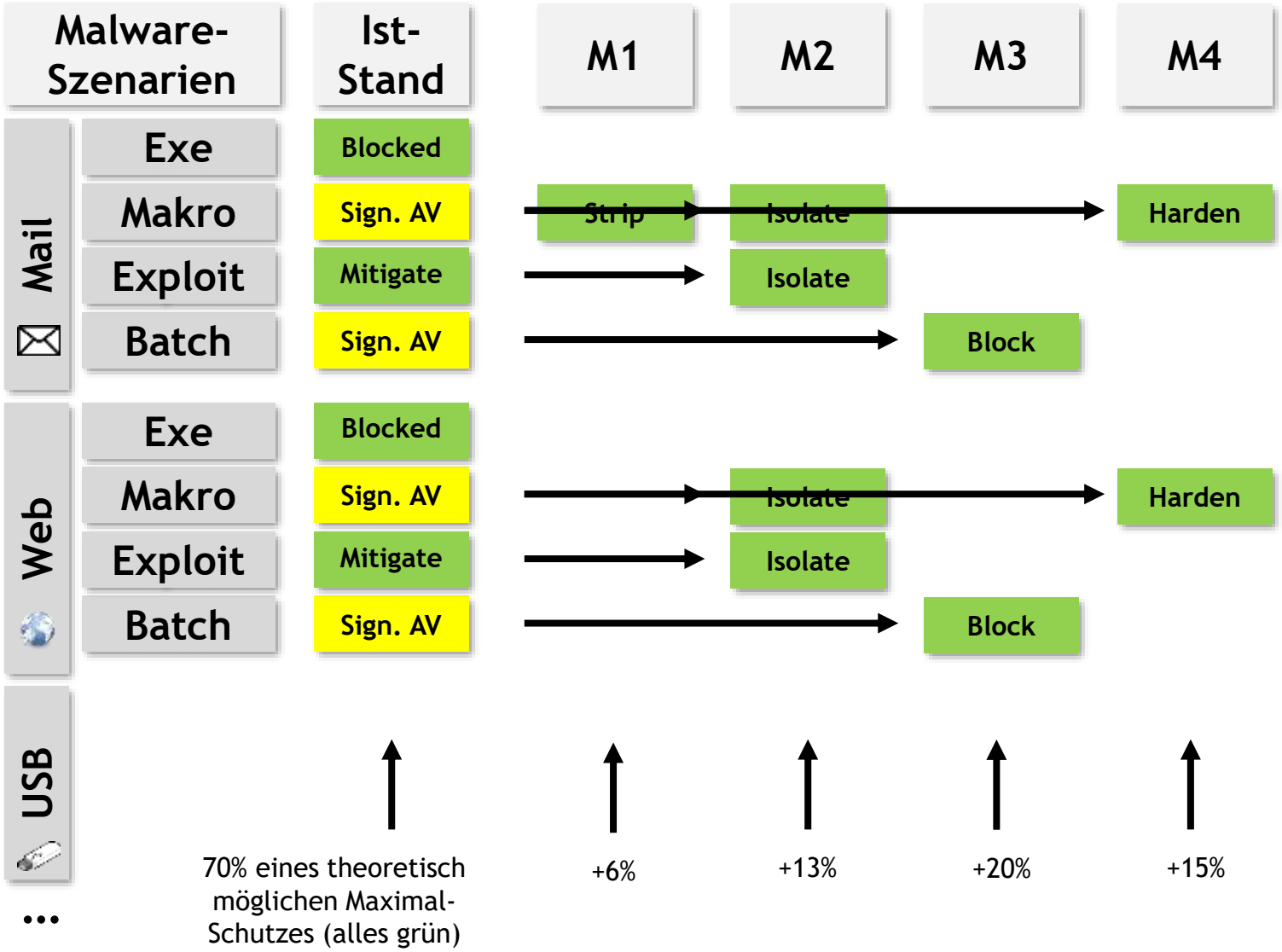
# Als Gesamt-Spalte zusammenführen (Maxima)

| | Malware-Szenarien | Ist-Stand |
|---|---|---|
| Mail | Exe | Blocked |
| | Makro | Sign. AV |
| | Exploit | Mitigate |
| | Batch | Sign. AV |
| Web | Exe | Blocked |
| | Makro | Sign. AV |
| | Exploit | Mitigate |
| | Batch | Sign. AV |
| USB | | |
| ... | | |

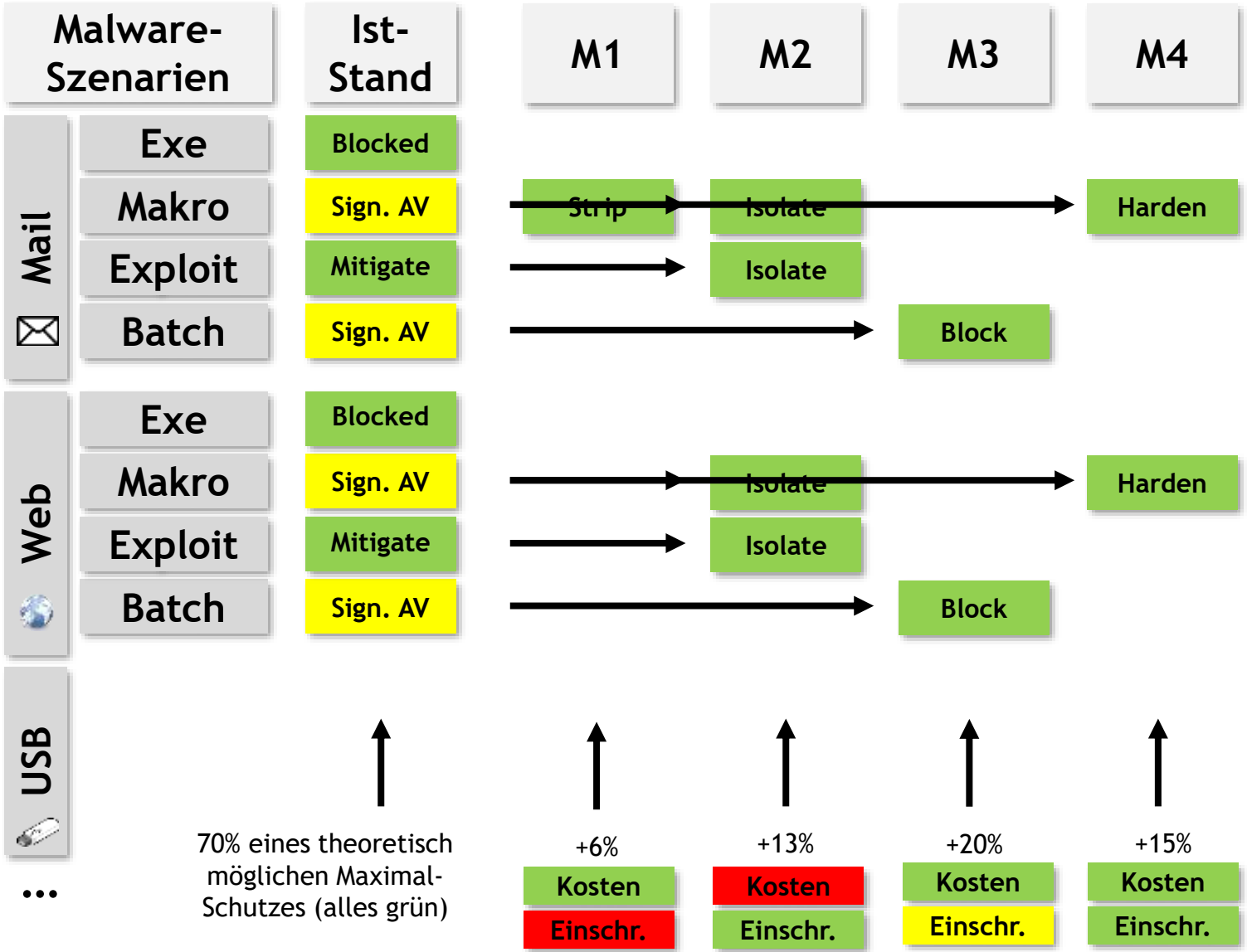
# Mögliche Maßnahmen und ihre jeweilige Verbesserung



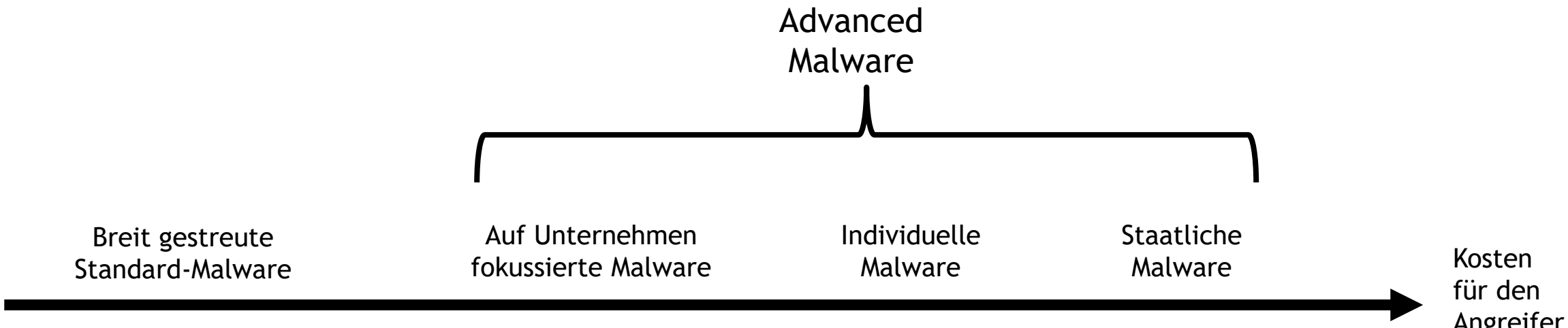
# Möglichkeiten zur Quantifizierung der Effekte



# Ergänzung der Kosten und Nebenwirkungen



# Qualität von Angriffen bzw. Malware



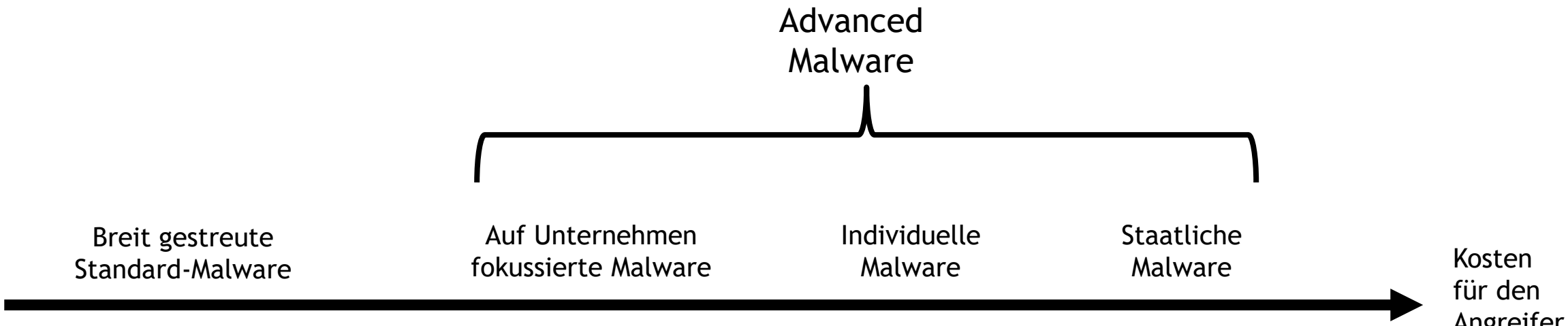

Zielen auf die Masse von Privatanwendern

- Um Geld von Konten zu stehlen
- Um durch Verschlüsselung von Daten Geld zu erpressen

Mit höherem Aufwand entwickelt bzw. von Profis gekauft

- Versucht Schutzmaßnahmen zu umgehen

# Qualität von Angriffen bzw. Malware

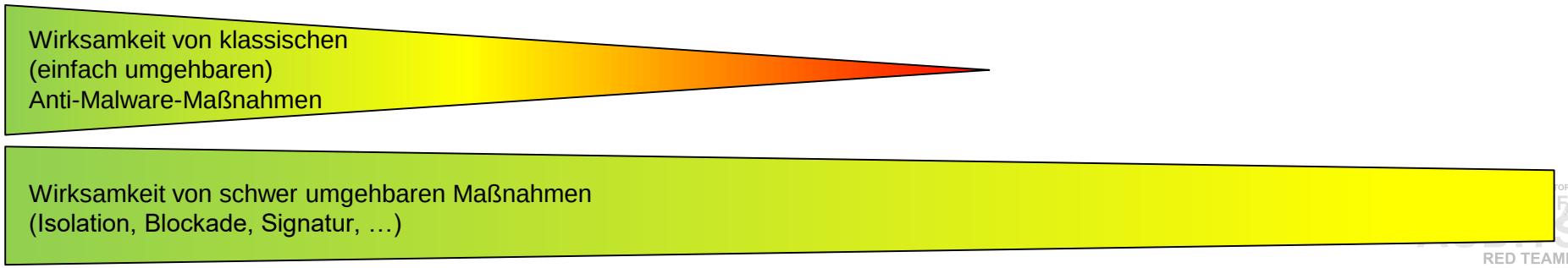



Zielen auf die Masse von Privatanwendern

- Um Geld von Konten zu stehlen
- Um durch Verschlüsselung von Daten Geld zu erpressen

Mit höherem Aufwand entwickelt bzw. von Profis gekauft

- Versucht Schutzmaßnahmen zu umgehen



# Differenzierte Bewertung von Maßnahmen

| | Malware-Szenarien | Mail GW | Web Proxy | EMET | App Locker |
|---|---|---|---|---|---|
| Mail | Exe | Blocked | Kein Schutz | Kein Schutz | Blocked |
| | Makro | Sign. AV | Kein Schutz | Kein Schutz | Kein Schutz |
| | Exploit | Sign. AV | Kein Schutz | Mitigate | Kein Schutz |
| | Batch | Sign. AV | Kein Schutz | Kein Schutz | Kein Schutz |
| Web | Exe | Kein Schutz | Sign. AV | Kein Schutz | Blocked |
| | Makro | Kein Schutz | Sign. AV | Kein Schutz | Kein Schutz |
| | Exploit | Kein Schutz | Sign. AV | Mitigate | Kein Schutz |
| | Batch | Kein Schutz | Sign. AV | Kein Schutz | Kein Schutz |
| | ... | ... | ... | ... | ... |
| USB | ... | | | | |

Wirksamkeit gegen einfache Malware

↓ Umgehbarkeit

Reduzierte Wirksamkeit gegen advanced Malware

# Differenzierte Bewertung von Maßnahmen

| Malware-Szenarien | | Mail GW | | Web Proxy | | EMET | | App Locker | |
|---|---|---|---|---|---|---|---|---|---|
| | | advanced | einfach | advanced | einfach | advanced | einfach | advanced | einfach |
| Mail | Exe | 4 | 4 | 0 | 0 | 0 | 0 | 3 | 4 |
| | Makro | 1 | 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Exploit | 1 | 2 | 0 | 0 | 2 | 3 | 0 | 0 |
| | Batch | 1 | 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| Web | Exe | 0 | 0 | 1 | 2 | 0 | 0 | 3 | 4 |
| | Makro | 0 | 0 | 1 | 2 | 0 | 0 | 0 | 0 |
| | Exploit | 0 | 0 | 1 | 2 | 2 | 3 | 0 | 0 |
| | Batch | 0 | 0 | 1 | 2 | 0 | 0 | 0 | 0 |
| ... | | ... | | ... | | ... | | ... | |
| USB | | | | | | | | | |
| ... | | | | | | | | | |

Wirksamkeit gegen einfache Malware

↓ Umgehbarkeit

Reduzierte Wirksamkeit gegen advanced Malware

cirosec

# Der typische Projektablauf

# Der typische Ablauf von Projekten zur Erstellung eines Malwareschutzkonzeptes

- Ermitteln der vorhandenen Maßnahmen zum Schutz vor Malware
  - Workshop + optionale Interviews / Vertiefungen
- Bewertung der bisherigen Situation unter Berücksichtigung der Wirksamkeiten
  - Darstellen der vorhandenen Lücken
- Ableiten von Maßnahmen, die vorhandene Lücken optimal schließen
- Sinnvolle Kombination und Konzeption
  - Mit verschiedenen Szenarien und Optionen

cirosec

# Fragen ?