Cyber Security – Alles im Griff?

Fachtagung 2017

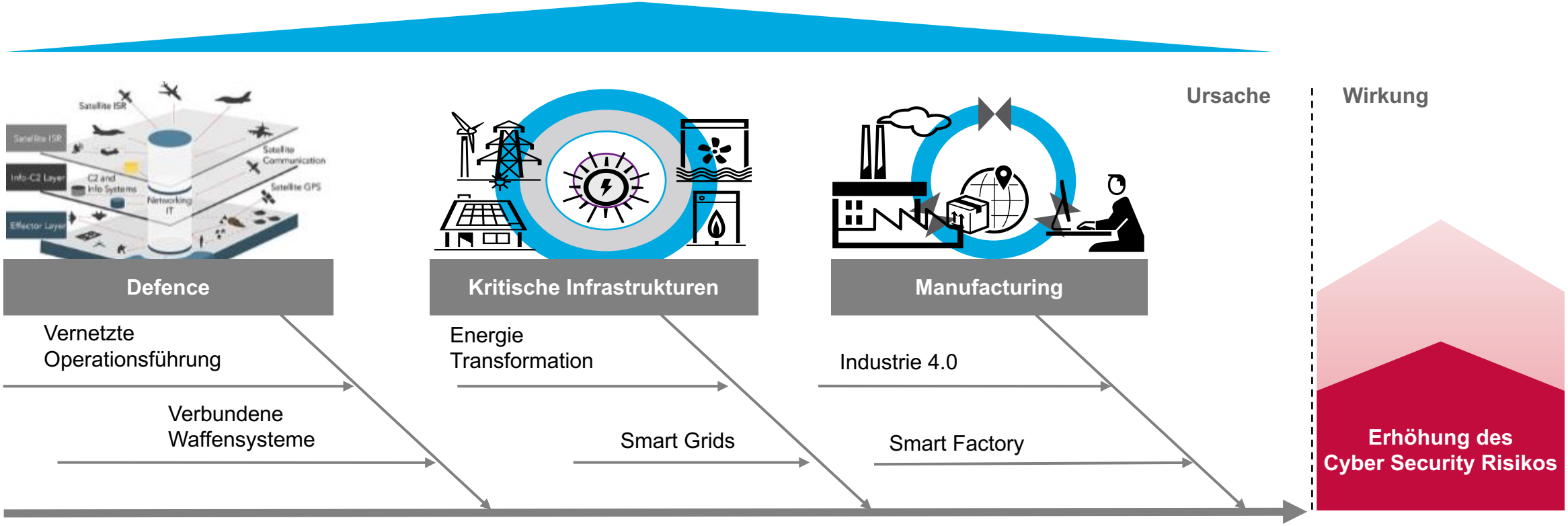
SZSV FSPC FSPC
Schweizerischer Zivilschutzverband
Fédération suisse de la protection civile
Federazione svizzera della protezione civile

René Bodmer
Director Sales Cyber Security
RUAG Defence
rene.bodmer@ruag.com

Together ahead. RUAG

Markt Treiber

Cyber Security ist das Topthema auf den Agenden der CxO!



Together ahead. RUAG

Ein Blick zurück – Historie der Malware-Entwicklung

1994

1

EIN NEUES VIRUS
PRO STUNDE

2006

1

EIN NEUES VIRUS
PRO MINUTE

2011

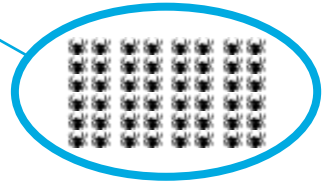
1

EIN NEUES VIRUS
PRO SEKUNDE

2016

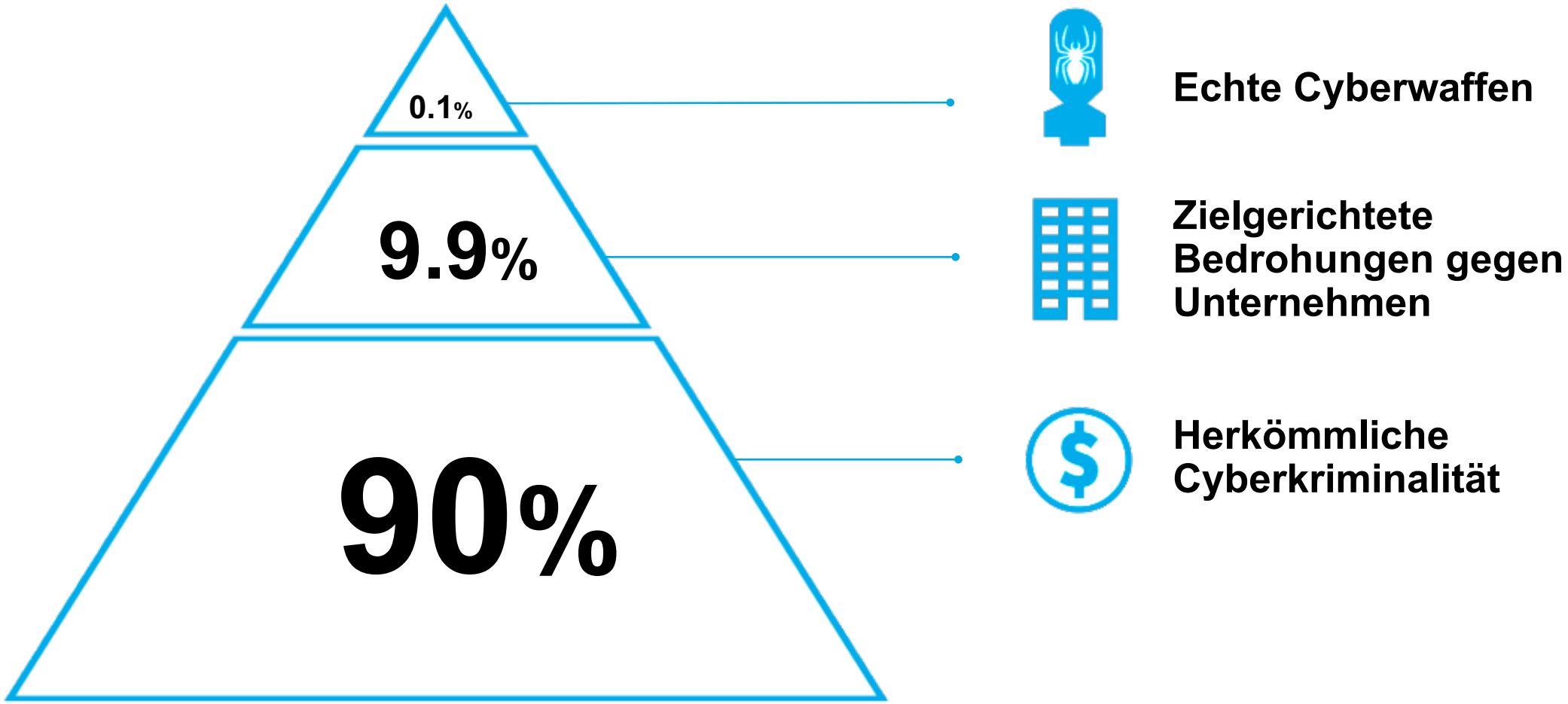
310’000

NEUE VARIANTEN
TÄGLICH



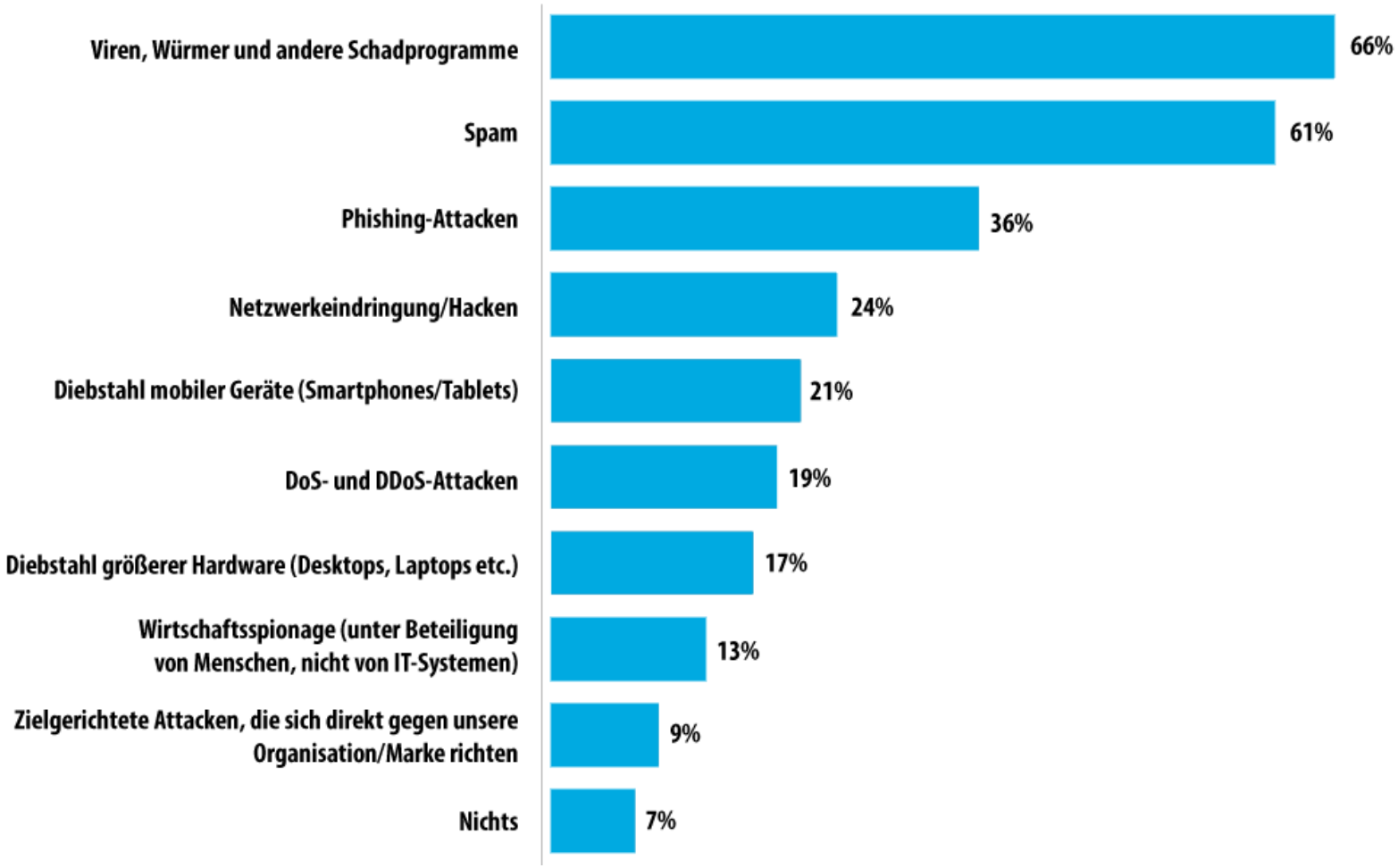
Together
ahead. RUAG

Malware heute



Together ahead. RUAG

Bedrohungslage aus Sicht von Unternehmen



Verbreitungswege

Together ahead. RUAG

Gründe für Attacken

- Datendiebstahl
- Datenvernichtung & -manipulation
- Gelddiebstahl
- Hacktivismus

Together ahead. RUAG

Planung der Angriffe

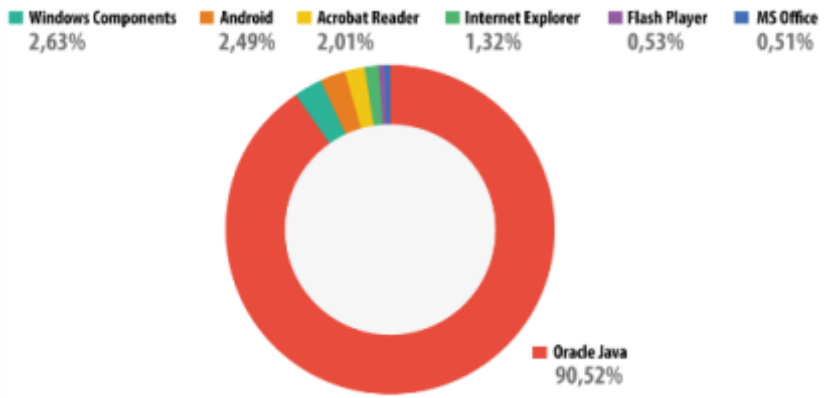
- Methoden
- Das schwächste Glied
- Social Engineering
- Sicherheitslücken

Wer muss sich schützen?

Together ahead. RUAG

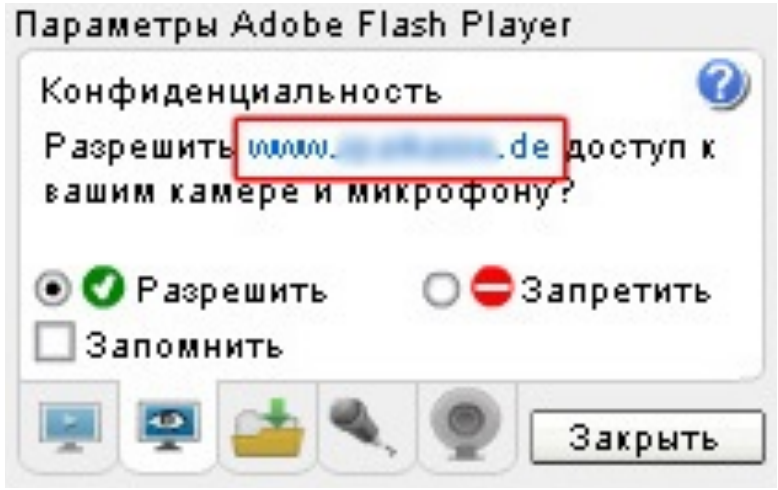
Technologien

- Diebstahl von Zertifikaten
- Sicherheitslücken
- Ransomware
- Weitere Plattformen



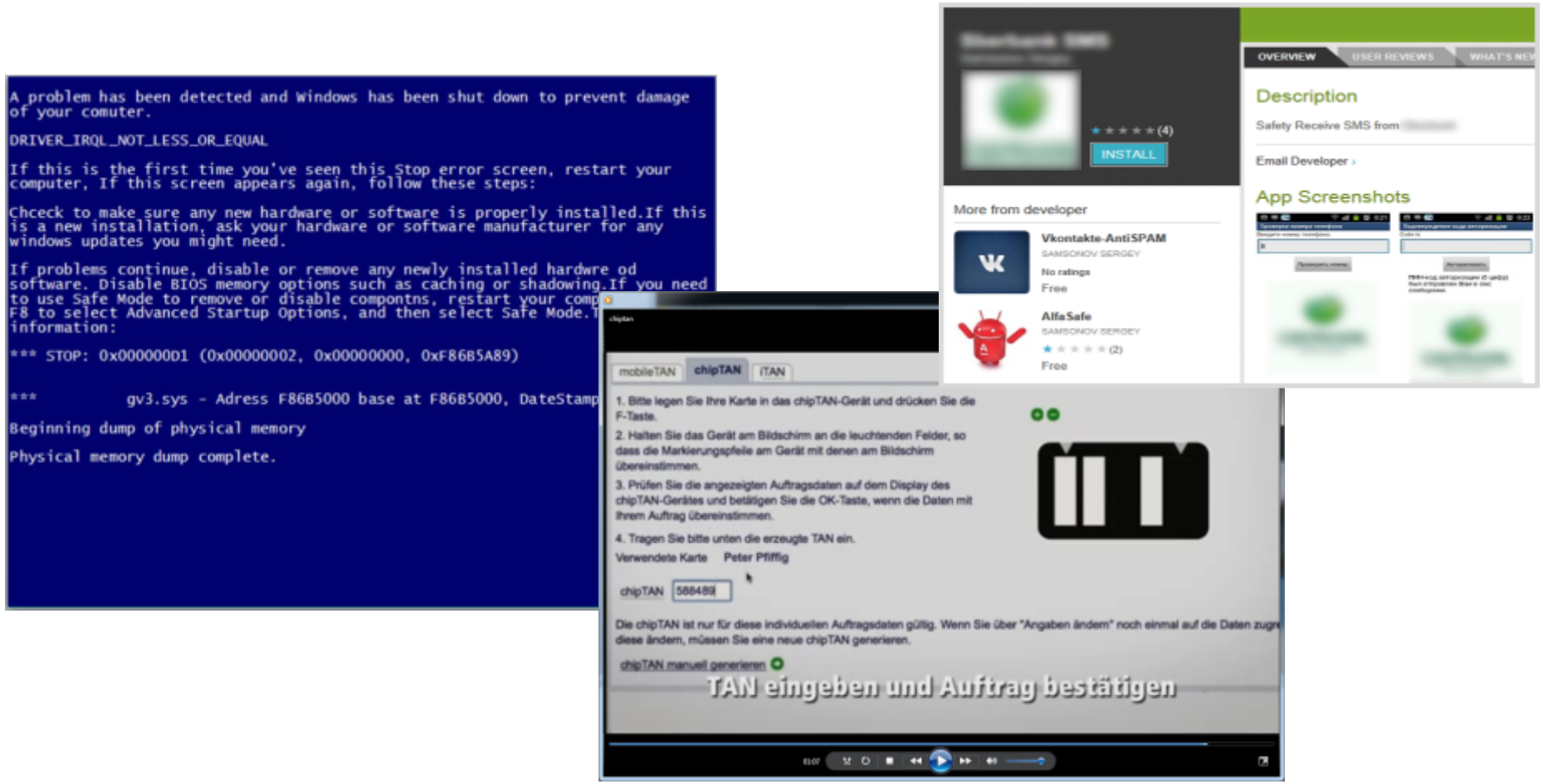
Together ahead. RUAG

Spyeye: Ausspionieren per Webcam



Together ahead. RUAG

Online Banking: Noch sicher?



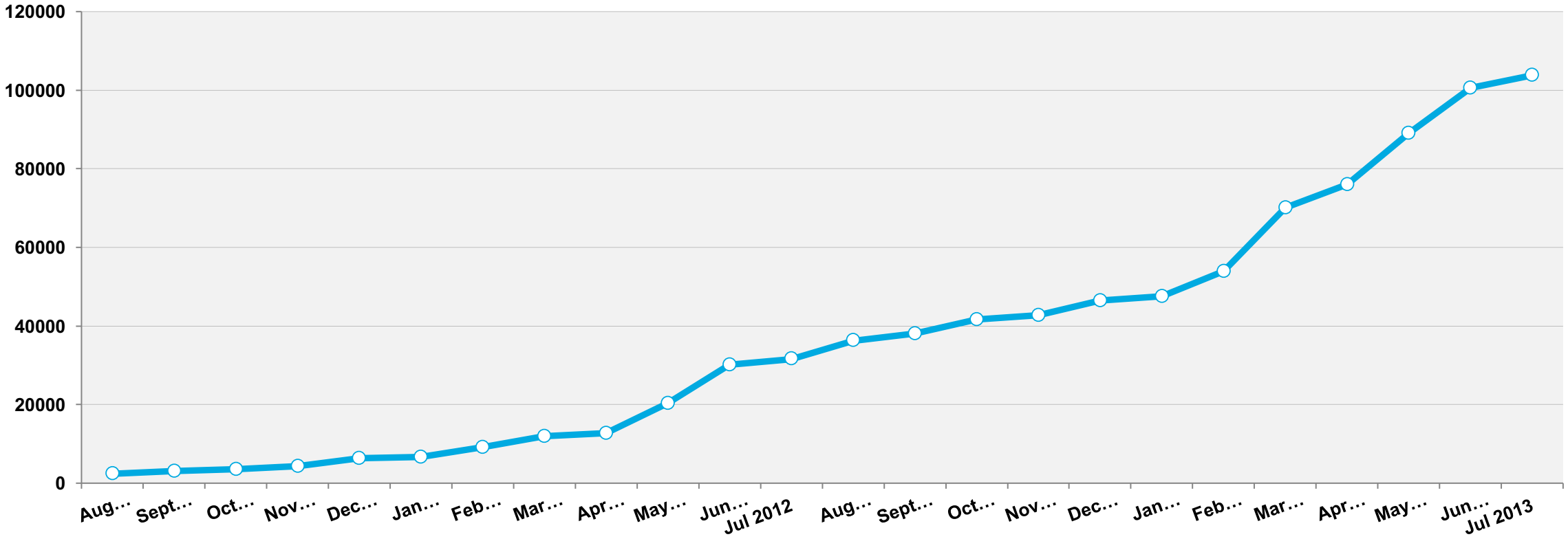
Together ahead. RUAG

Ziel: Mobiltelefon – Weshalb?

- eingehende und ausgehende SMS-Nachrichten
- Arbeits-E-Mails
- Geschäfts-kontakte
- persönliche Fotos
- GPS-Koordinaten
- Anmeldedaten für das Online-Banking
- Kalender
- verschiedene installierte Apps

Malware-Varianten bei mobilen Geräten

Anzahl einzigartiger Varianten



Together ahead. RUAG

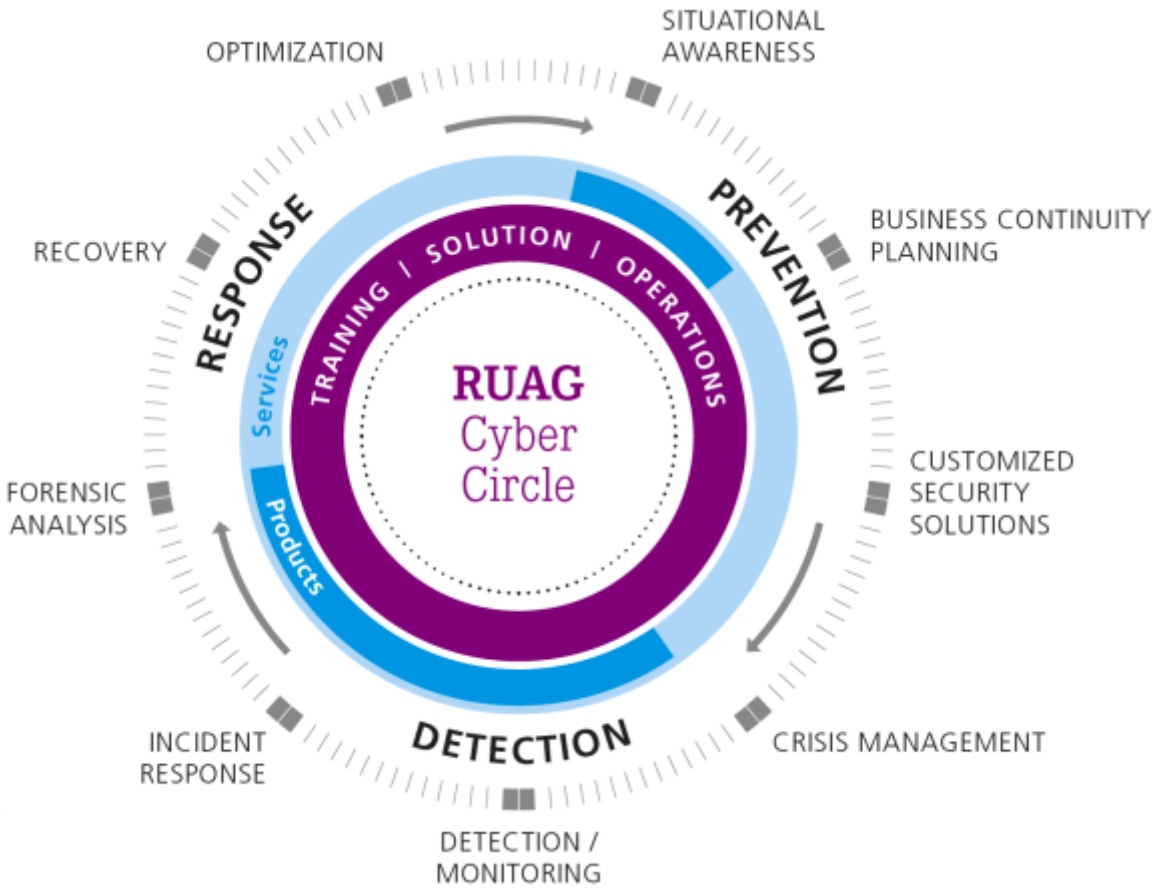
Prognosen

- Mobile Bedrohungen
- Bitcoin
- Angriffe auf Cloud-Speicher
- Cybersöldner

Together ahead. RUAG

Überlebensfähigkeit im Cyberspace

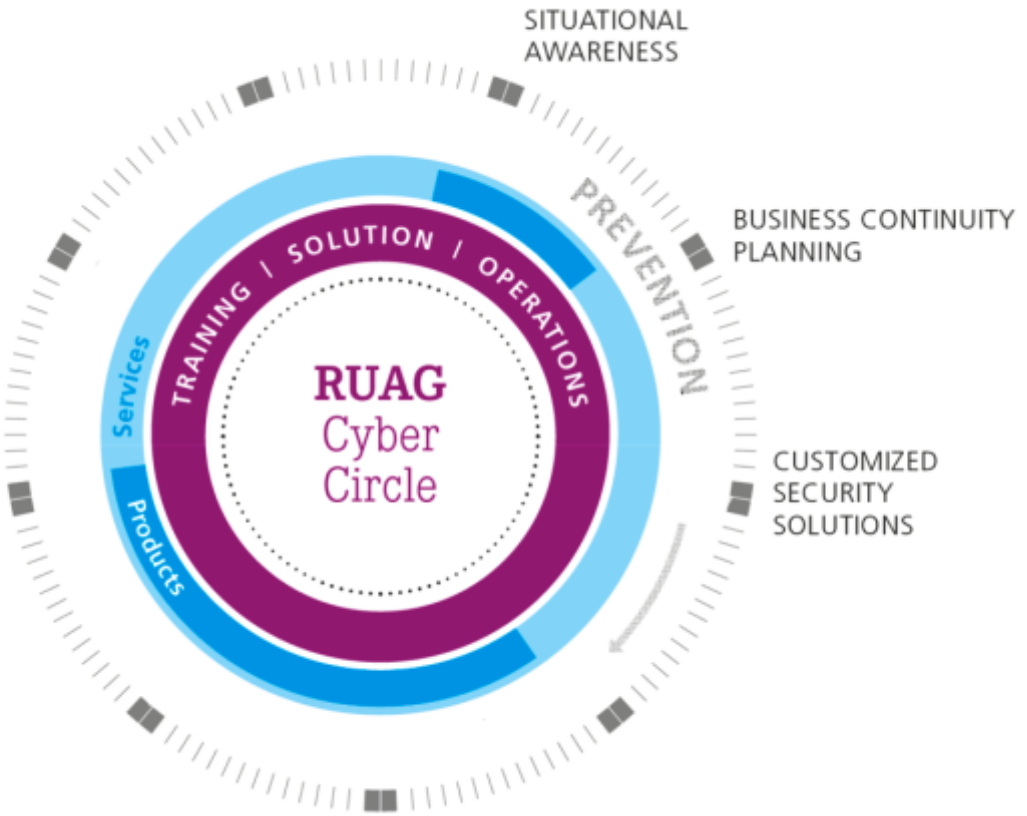
- **Vor dem Angriff**
  - Situational Awareness gewinnen
  - Schutzbedarf definieren
  - Systeme härten
- **Während des Angriffs**
  - Angriffe früh erkennen
  - Resilienz aufrecht erhalten
  - Durch die Krise führen
- **Nach dem Angriff**
  - Beweise sichern
  - Wiederherstellung der Leistungsfähigkeit
  - Aus Angriff lernen



Together ahead. RUAG

Gegenmassnahmen – Prevention

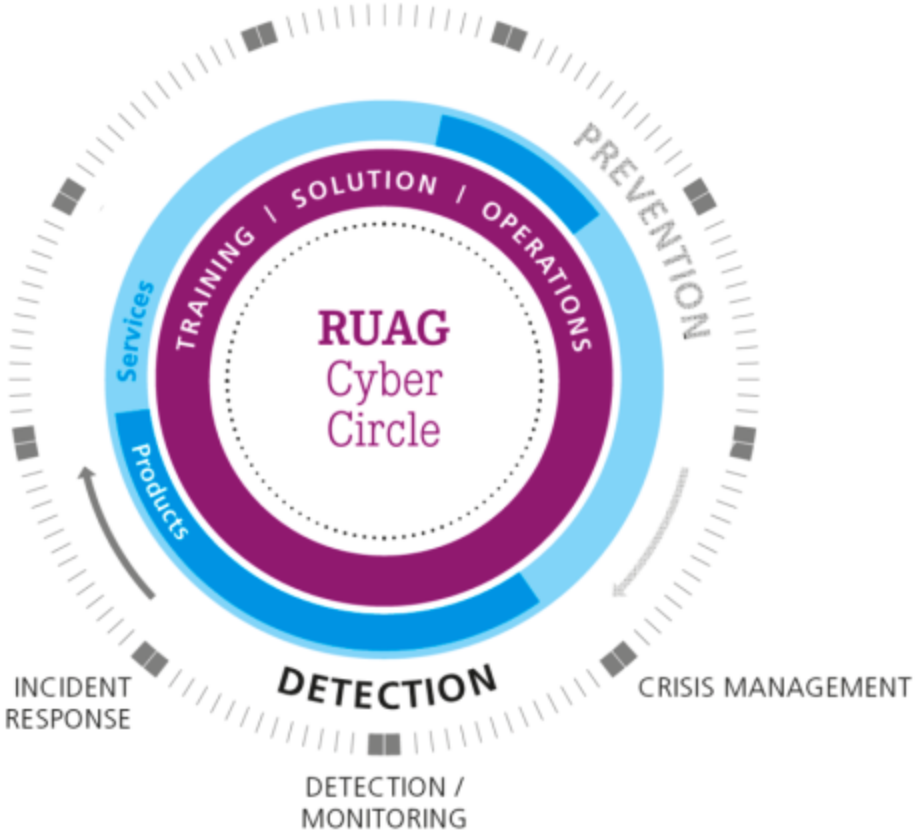
- Möglichkeiten des Angreifers kennen
- Risiken und Schutzobjekte identifizieren
- Systeme härten
- Infektion vermeiden
- Mitarbeitende sensibilisieren



Together ahead. RUAG

Gegenmassnahmen – Detection

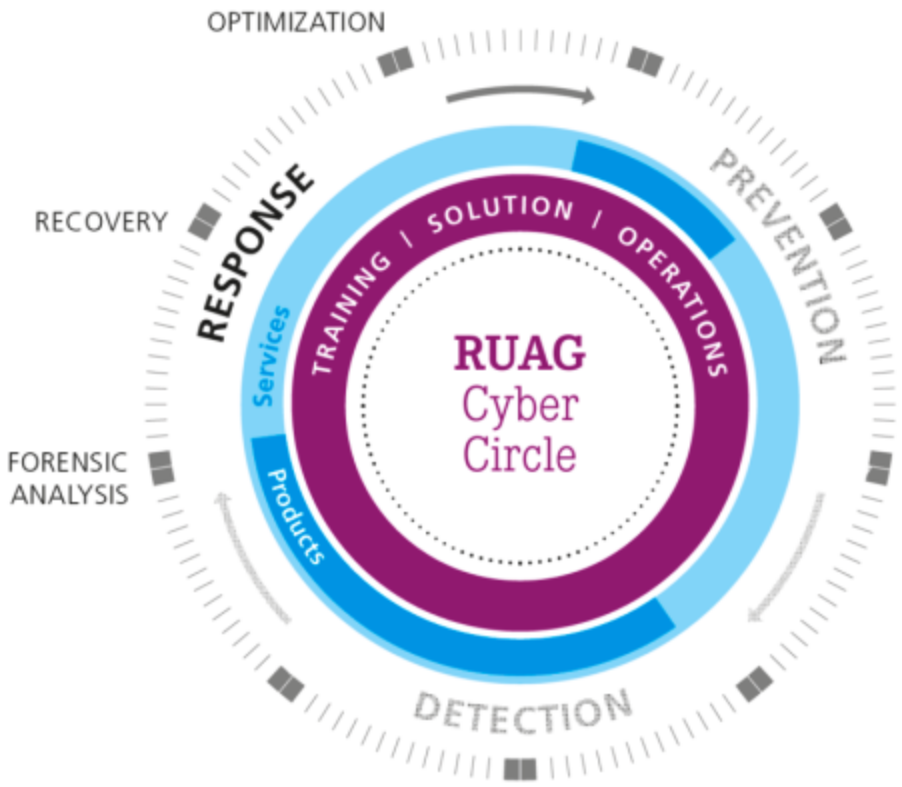
- Angriffe früh erkennen
- Art des Angriffs bestimmen
- Betroffene Systeme isolieren
- Sofortmassnahmen einleiten
- Durch die Krise führen



Together
ahead. RUAG

Gegenmassnahmen – Response

- Schaden analysieren
- Beweise sichern
- Systeme wiederherstellen
- Sicherheitslücken schliessen
- Aus Angriff lernen



Together ahead. RUAG

Erkenntnisse

- Cyber Operationen sind gut geplant und geführt!
- Der Angriff erfolgt in Phasen und über längere Zeit
- Die Gegner denken in Effekten
- Der Notfall-/Krisenstab muss auch in Effekten denken
  (Prozesse und Kommunikation sind permanent zu überprüfen und trainieren)
- Keine Irritation aufgrund der technischen Komplexität zulassen
- Know-How Austausch und Vernetzung sind sicherzustellen
  (u.a. Swiss Cyber Experts, Security SIGS, Cyber Sicherheitsrat e.V.)

Vielen Dank für Ihre Aufmerksamkeit

René Bodmer
Director Sales Cyber Security
RUAG Defence
rene.bodmer@ruag.com

Together ahead. RUAG