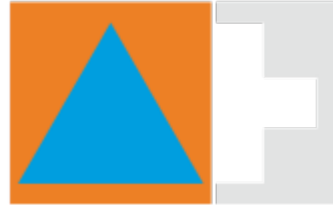


# Cyber Security – Alles im Griff?

**Fachtagung 2017**



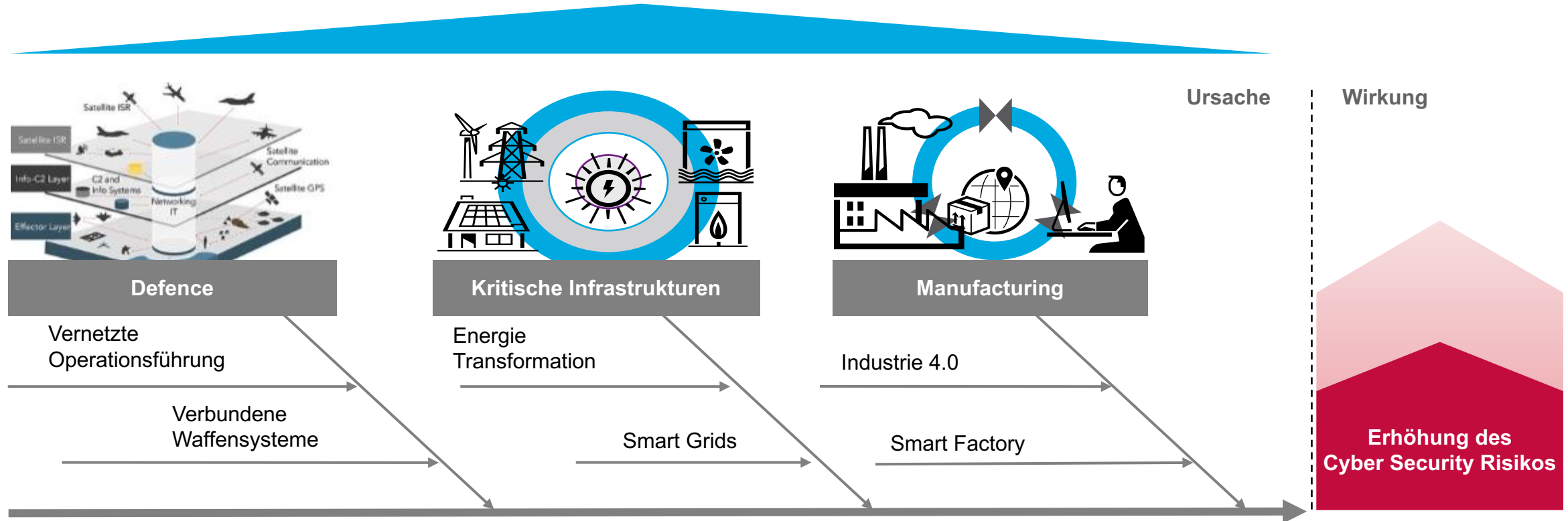
**SZSV**  
**FSPC**  
**FSPC**

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

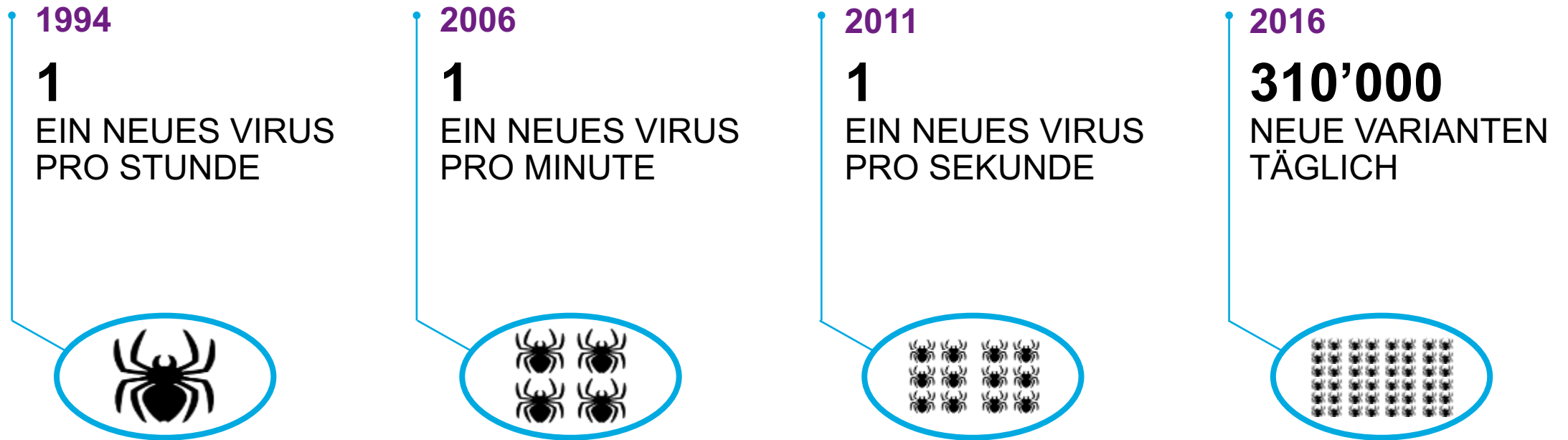
René Bodmer  
Director Sales Cyber Security  
RUAG Defence  
[rene.bodmer@ruag.com](mailto:rene.bodmer@ruag.com)

# Markt Treiber

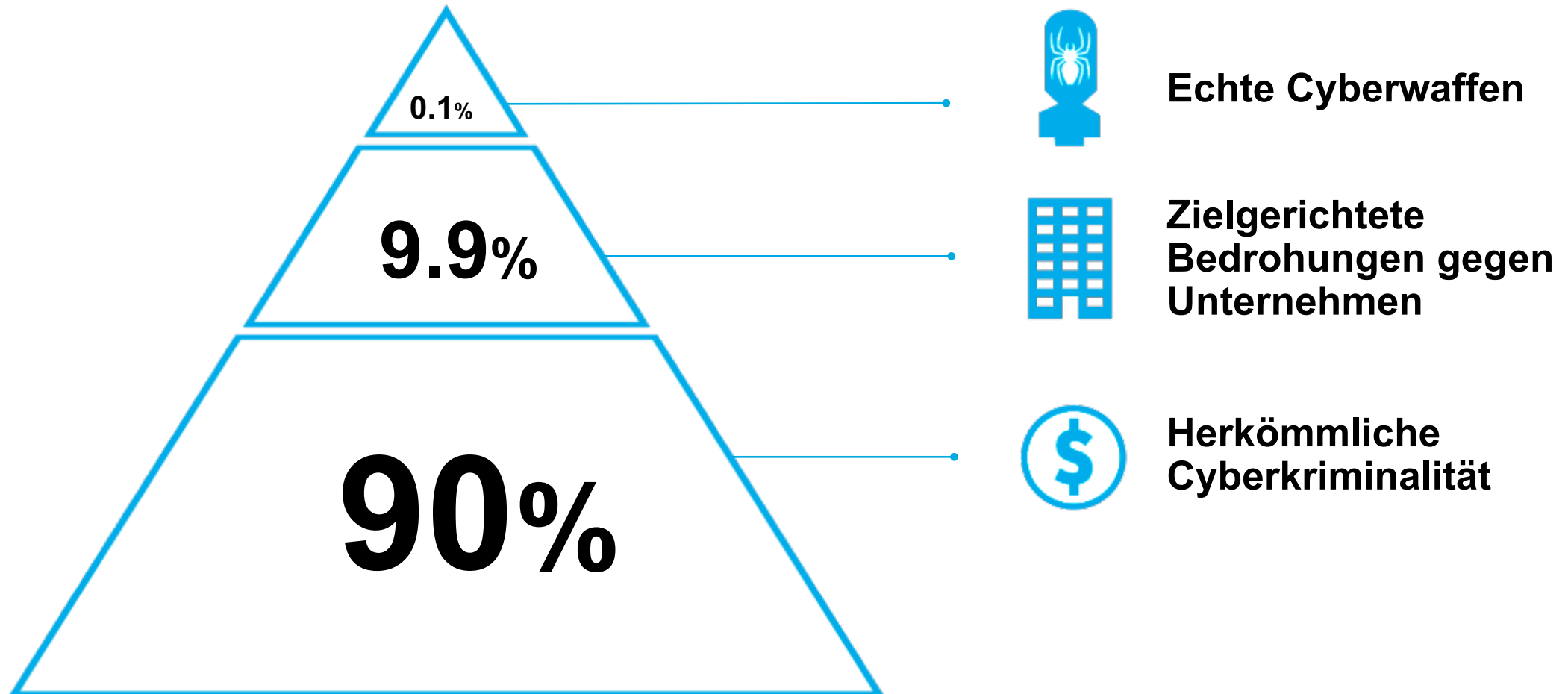
Cyber Security ist das Topthema auf den Agenden der CxO!



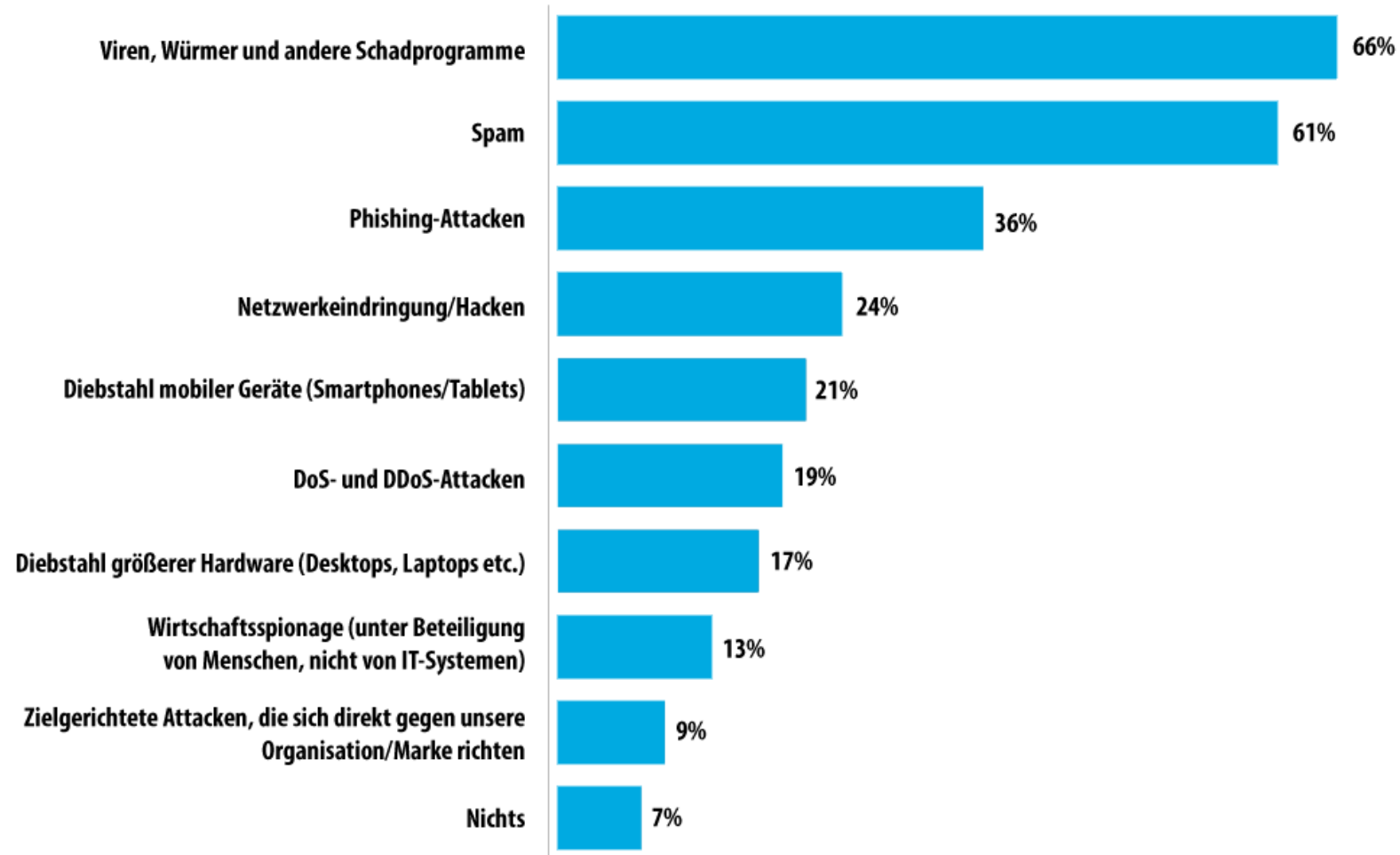
# Ein Blick zurück – Historie der Malware-Entwicklung



# Malware heute



# Bedrohungslage aus Sicht von Unternehmen



# Verbreitungswege



# Gründe für Attacken

- Datendiebstahl
- Datenvernichtung & -manipulation
- Gelddiebstahl
- Hacktivismus

The screenshot displays a grid of eight product cards, each representing a different financial institution or network. Each card includes the logo, a price per unit, a 'Warranty' (3-day), and 'Min buy' and 'Max buy' quantities. Below each card is a 'Buy now' button and a 'quantity' or 'Buy With Balance' option.

Product	Price per Unit	Warranty	Min Buy	Max Buy	In Stock	Buy With
Visa Cw	2 \$	3 day	5	30	42	quantity
Master Cw	2.5 \$	3 day	5	30	42	quantity
Discover Cw	3.5 \$	3 day	5	30	42	quantity
Amex Cw	3.5 \$	3 day	5	30	42	quantity
Bank of America	50\$	3 day	1	3	13	Balance
Citibank	50\$	3 day	5	30	42	Balance
HSBC	50\$	3 day	5	30	42	Balance
Regions	50\$	3 day	5	30	42	Balance



Together  
ahead. **RUAG**

# Planung der Angriffe

- Methoden
- Das schwächste Glied
- Social Engineering
- Sicherheitslücken





# Wer muss sich schützen?



Adressen

### Adressen-Datenblatt

Adress-Kennzeichen: PS   negativ

Adr-Nr.	7	Kunden-Nr.		Geburtsdatum		Datum letzter Besuch	04.02.2013
Anrede	Familie	Titel		Geburtsjahr		Bezugnahme durch	
Name/Firma	Mustermann			Telefon		Notfall Ansprechpartner	
Vorname	Max			Mobil-Telefon		Name	
Zusatzname				Fax		Telefon	
PLZ Ort	01234	Dresden		E-Mail Eingabe			
Straße				Anwendung		l.g.schmidt@t-online.de	
Anmerkungen							

**Tiere** Rabatt 0% alle Tiere zur Adr.: Otto Bello

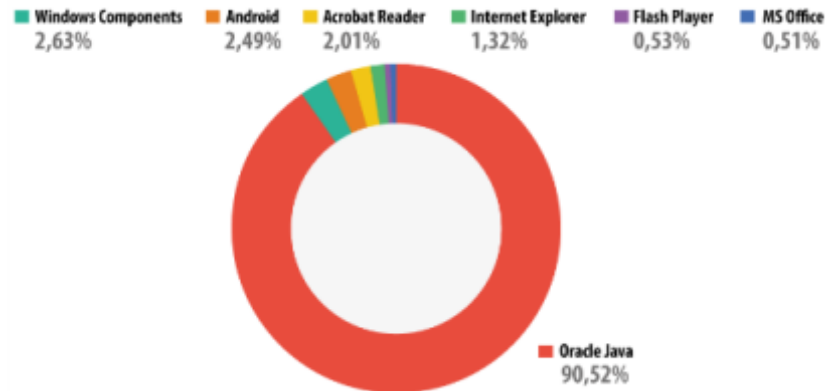
TierNr.	9	Merkmale	
Tierart	Katze	Auswahl	
Tiername	Otto	Krankheiten	
Rasse	Perserkatze	Medikamente	
Mischung		Auswahl	
Geburtsdatum		Fütterung	
Geburtsjahr		keine Besonderheiten	
Größenkl.	Tagesgebühr	Auswahl	
kastriert	unverträglich	Bilddatei	
Übernahme		C:\Users\Schmidt\Pictures\Bilder\Morli.JPG	
Chip/Tatow		Vorbesitzer	Tierarzt
Anmerkungen		Versicherung	Verbleib Ableben

Together  
ahead. **RUAG**



# Technologien

- Diebstahl von Zertifikaten
- Sicherheitslücken
- Ransomware
- Weitere Plattformen



**Die offizielle Mitteilung der Bundeskriminalamt**

**BUNDESPOLIZEI** Bundeskriminalamt

**Ukash** dedede OK

### Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).

Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

**Tankstellen** - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

**epay** - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

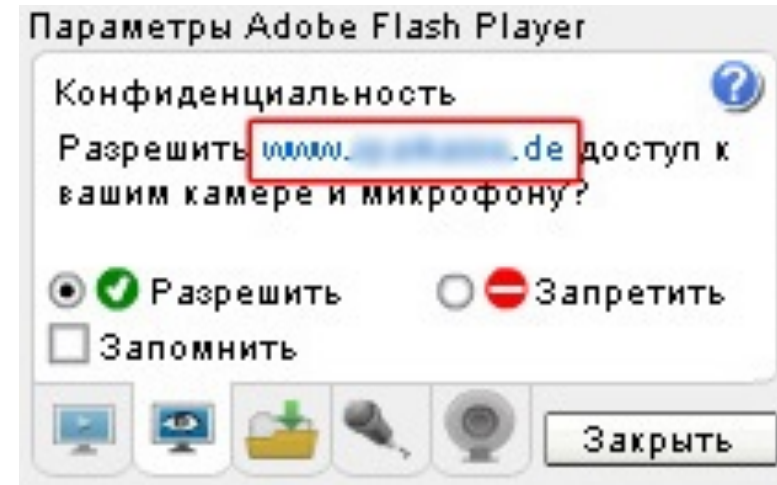
**Achtung!**  
Ein Vorgang illegaler Aktivitäten wurde erkannt.  
Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet "82.254.165.159" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sadomie und Gewalt gegen Kinder aufgerufen.  
Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!  
Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperrung des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.  
Ihre Daten:  
**IP:** 82.254.165.159  
**Browser:** Internet Explorer 7.0  
**OS:** Windows XP  
**Das Land:** FRANCE  
**City:** ...  
**ISP:** ...

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen. Die Zahlung ist innerhalb von 24 Stunden zu leisten. Sollte der Eingang der Zahlung in der vorgegebenen Zeit nicht erfolgen, so wird Ihre Festplatte unwiderruflich formatiert/ gelöscht.  
Die Bezahlung erfolgt durch einen Ukash Coupon-Code in Höhe von 100 Euro.  
Um die Bezahlung durchzuführen, geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschließend auf OK)  
Sollte das System Fehler melden, so müssen Sie den Code per Email (.....@yahoo.com) versenden.  
Nach Eingang der Zahlung wird Ihr Computer innerhalb von 24 Stunden wieder freigestellt.

2010 - 2011 © Der Service des Dienstes des Internet der Sicherheit ist mit der Unterstützung der Gesellschaften entwickelt.

McAfee symantec Kaspersky Microsoft

# Spyeye: Ausspionieren per Webcam



# Online Banking: Noch sicher?

```
A problem has been detected and windows has been shut down to prevent damage of your computer.  
DRIVER_IRQL_NOT_LESS_OR_EQUAL  
If this is the first time you've seen this Stop error screen, restart your computer, If this screen appears again, follow these steps:  
Check to make sure any new hardware or software is properly installed.If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.  
If problems continue, disable or remove any newly installed hardware od software. Disable BIOS memory options such as caching or shadowing.If you need to use Safe Mode to remove or disable compontns, restart your comp. F8 to select Advanced Startup Options, and then select Safe Mode.  
Information:  
*** STOP: 0x000000D1 (0x00000002, 0x00000000, 0xF86B5A89)  
  
***      gv3.sys - Adress F86B5000 base at F86B5000, DateStamp  
Beginning dump of physical memory  
Physical memory dump complete.
```

AlfaSafe  
SAMSONOV SERGEY  
★ ★ ★ ★ (4)  
INSTALL

More from developer

Vkontakte-AntiSPAM  
SAMSONOV SERGEY  
No ratings  
Free

AlfaSafe  
SAMSONOV SERGEY  
★ ★ ★ ★ (2)  
Free

OVERVIEW USER REVIEWS WHAT'S NEW

Description  
Safety Receive SMS from [redacted]

Email Developer >

App Screenshots

mobileTAN chipTAN iTAN

- Bitte legen Sie Ihre Karte in das chipTAN-Gerät und drücken Sie die F-Taste.
- Halten Sie das Gerät am Bildschirm an die leuchtenden Felder, so dass die Markierungspfeile am Gerät mit denen am Bildschirm übereinstimmen.
- Prüfen Sie die angezeigten Auftragsdaten auf dem Display des chipTAN-Gerätes und betätigen Sie die OK-Taste, wenn die Daten mit Ihrem Auftrag übereinstimmen.
- Tragen Sie bitte unten die erzeugte TAN ein.

Verwendete Karte Peter Piffig

chipTAN 588489

Die chipTAN ist nur für diese individuellen Auftragsdaten gültig. Wenn Sie über "Angaben ändern" noch einmal auf die Daten zugre diese ändern, müssen Sie eine neue chipTAN generieren.

chipTAN manuell generieren

**TAN eingeben und Auftrag bestätigen**

# Ziel: Mobiltelefon – Weshalb?



eingehende und  
ausgehende SMS-  
Nachrichten



GPS-  
Koordinaten



Arbeits-  
E-Mails



Anmeldedaten für das  
Online-Banking



Geschäfts-  
kontakte



Kalender



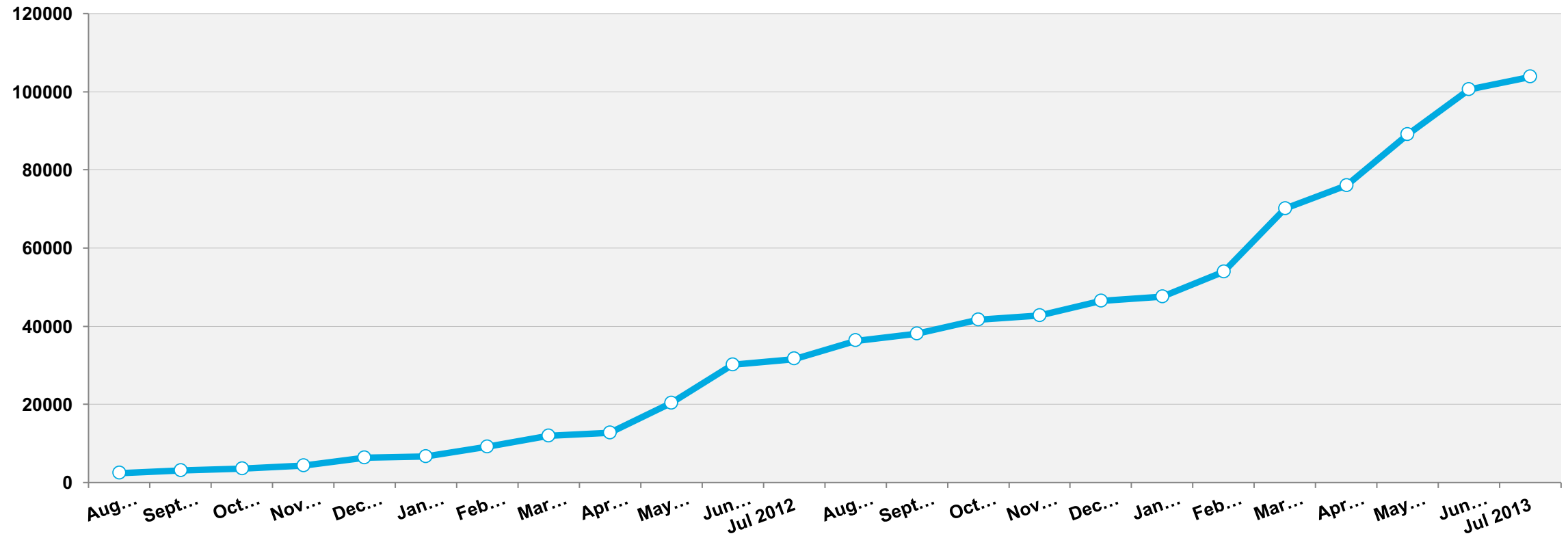
persönliche  
Fotos



verschiedene  
installierte Apps

# Malware-Varianten bei mobilen Geräten

Anzahl einzigartiger Varianten



# Prognosen

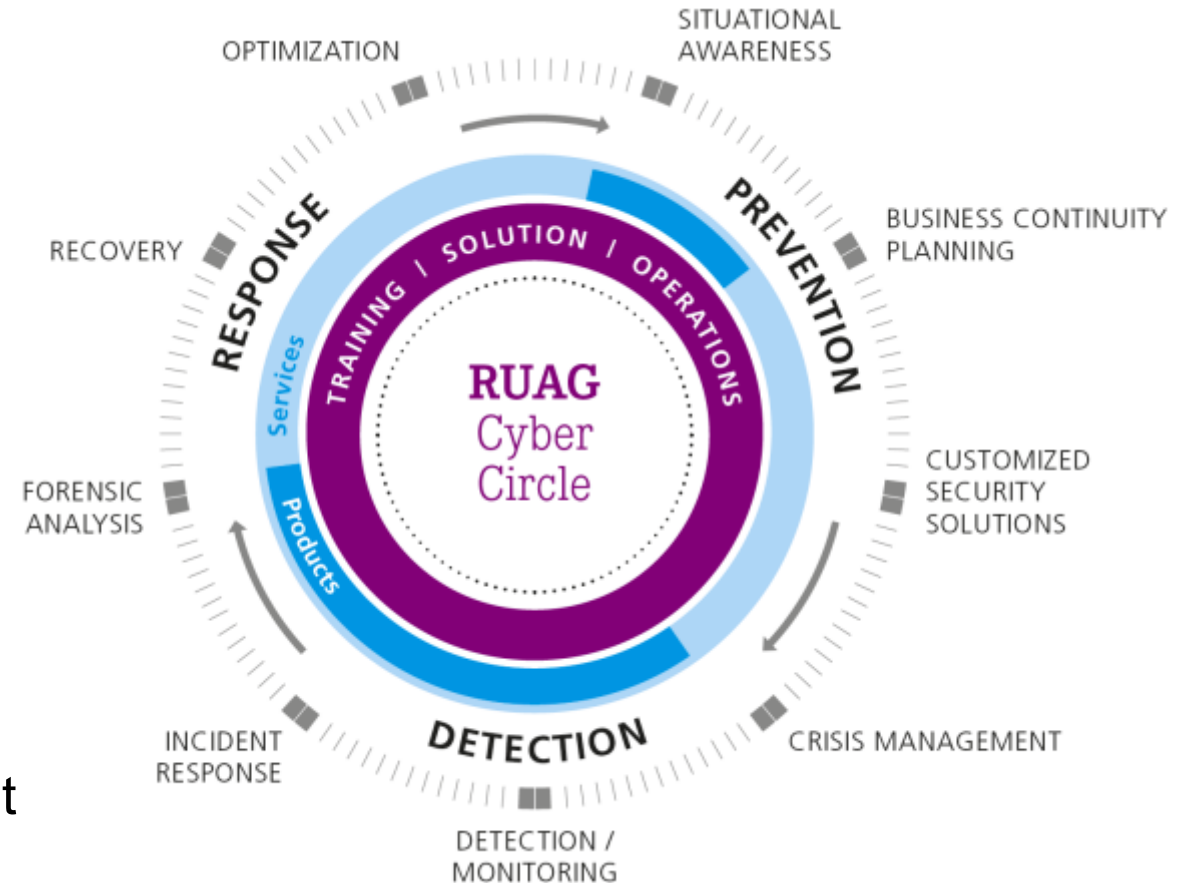
- Mobile Bedrohungen
- Bitcoin
- Angriffe auf Cloud-Speicher
- Cybersöldner





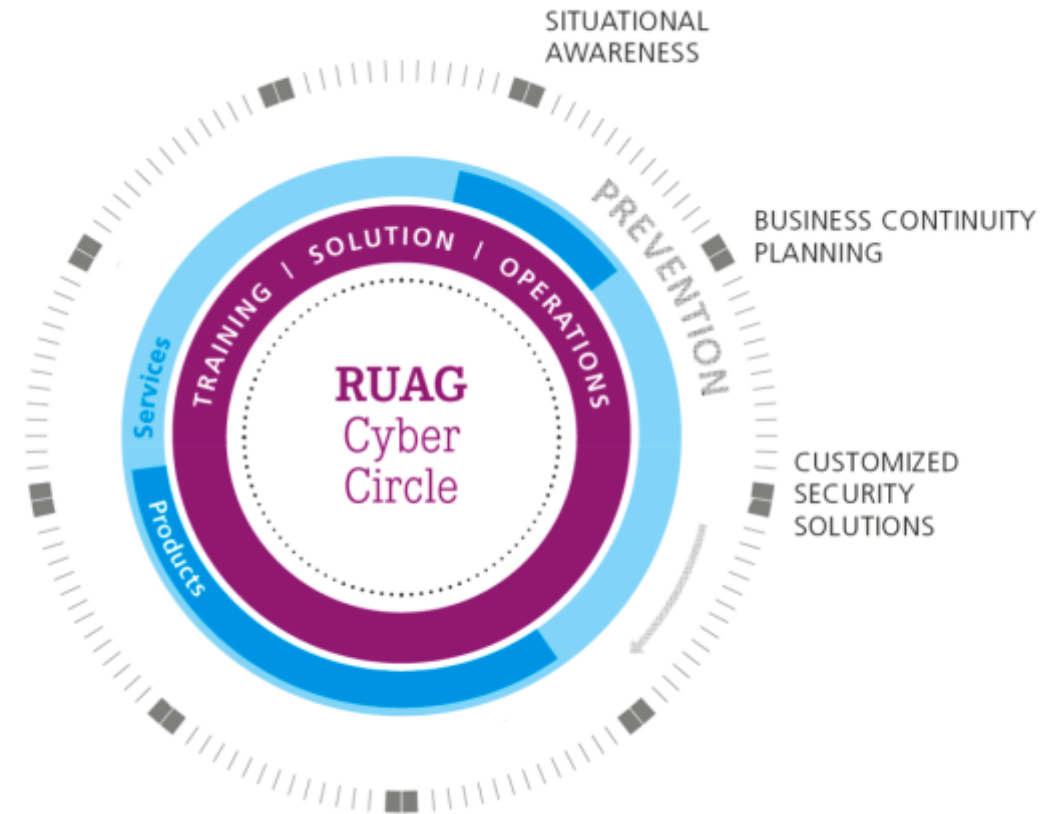
# Überlebensfähigkeit im Cyberspace

- **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



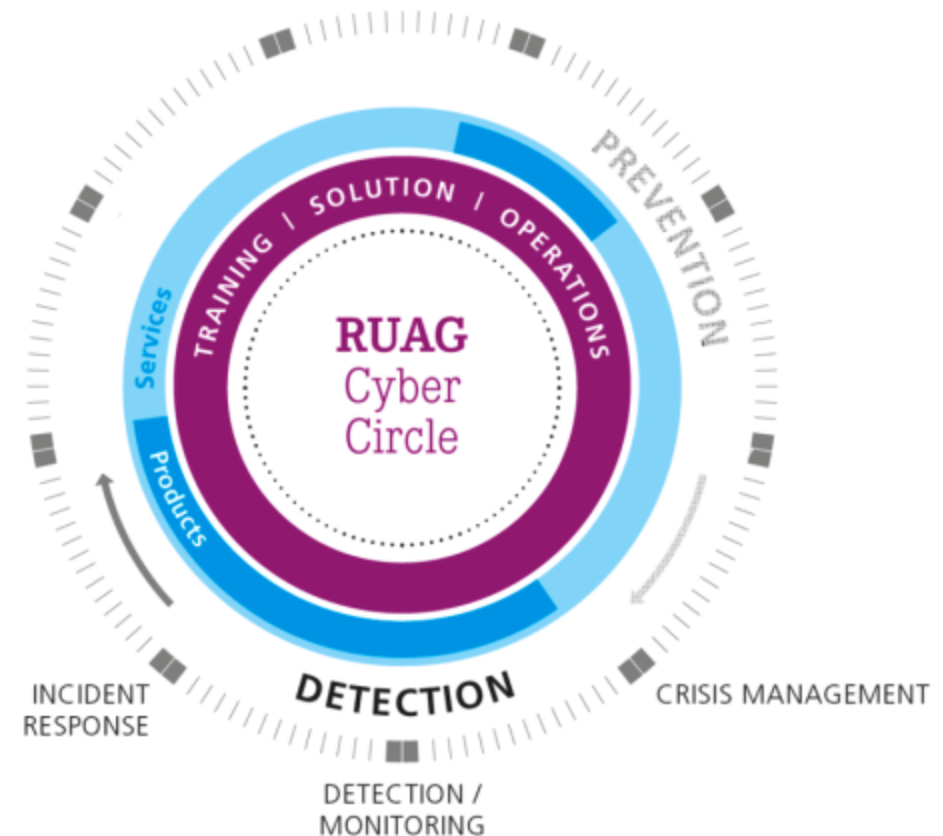
# Gegenmassnahmen – Prevention

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



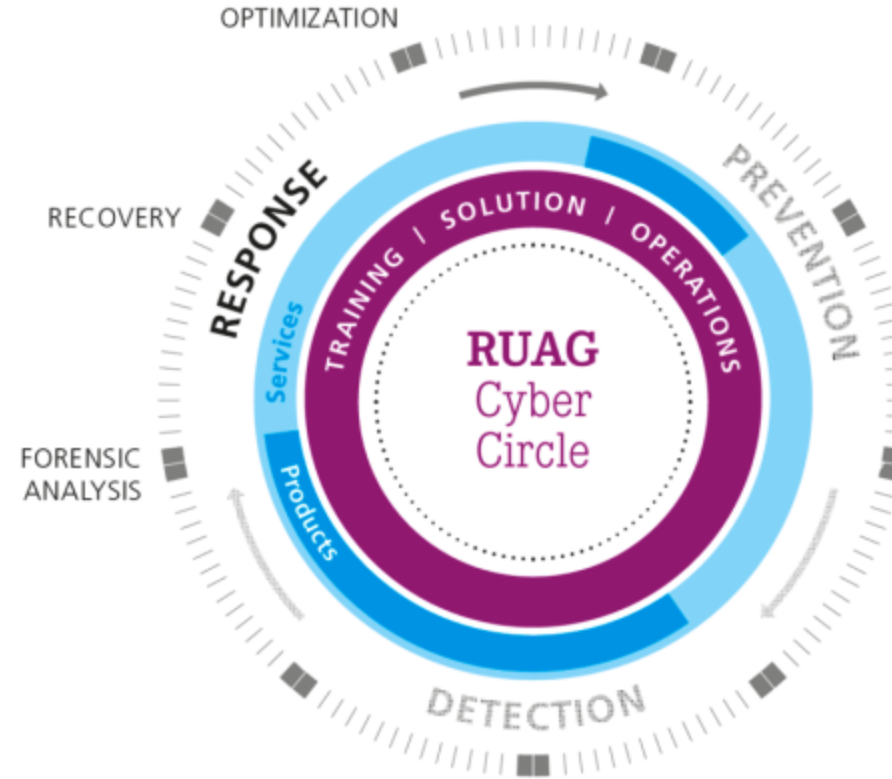
# Gegenmassnahmen – Detection

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



# Gegenmassnahmen – Response

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



# 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](mailto:rene.bodmer@ruag.com)

