



# Anatomie von IT-Angriffen

Wie in Firmennetze eingebrochen wird  
und was wir daraus lernen können

Immanuel Hoos

Externer Referent & Technischer Consultant

Symantec (Deutschland) GmbH, Symantec (Austria) GmbH, Symantec Switzerland AG



***Hans-Peter Friedrich (CSU)***

*Bundesinnenminister*

“*Es gibt massive Versuche, den  
“Rohstoff Geist” in deutschen  
Unternehmen zu stehlen.*”

Quelle: Welt kompakt vom 29. August 2013

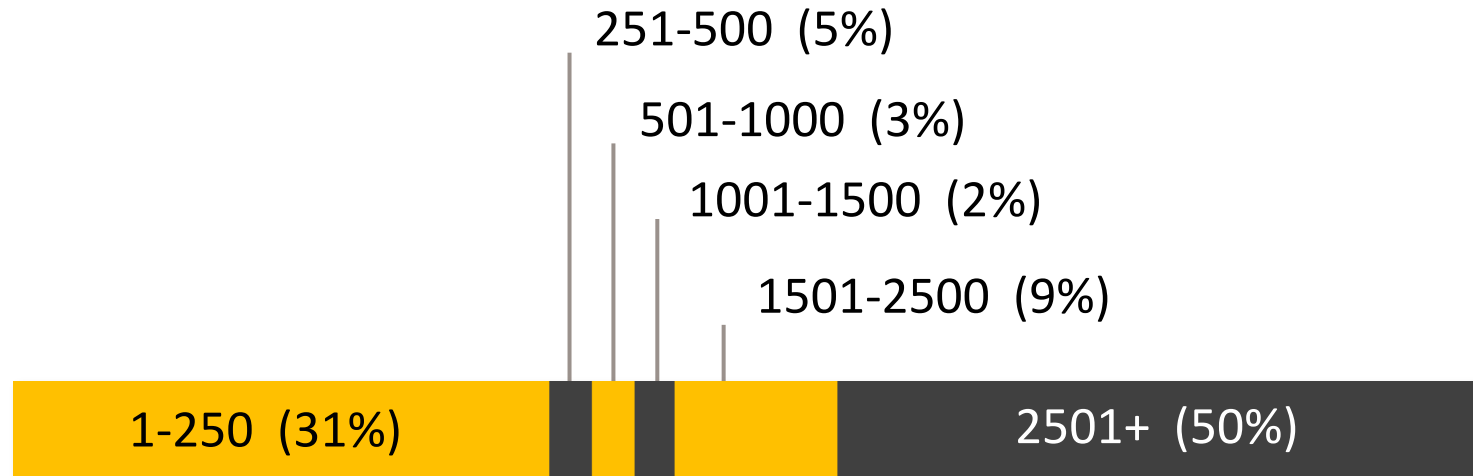
1 Daten und Fakten

2 Gezielte Angriffe

3 Gewöhnliche Angriffe

4 Maßnahmen

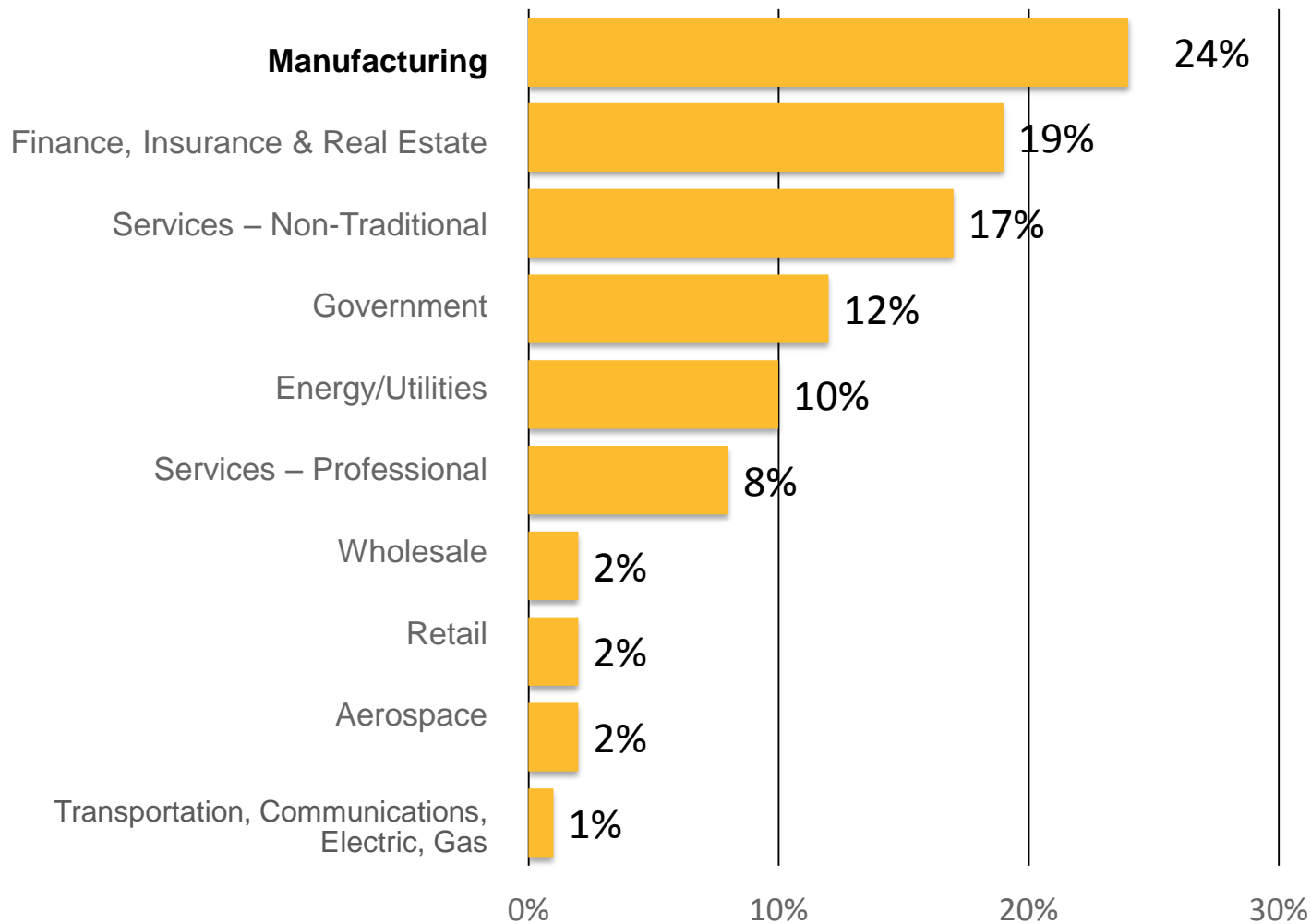
# Gezielte Angriffe nach Unternehmensgröße



Anzahl Mitarbeiter der angegriffenen Firma

Quelle: Internet Security Threat Report, Symantec 2013

# Gezielte Angriffe nach Branche



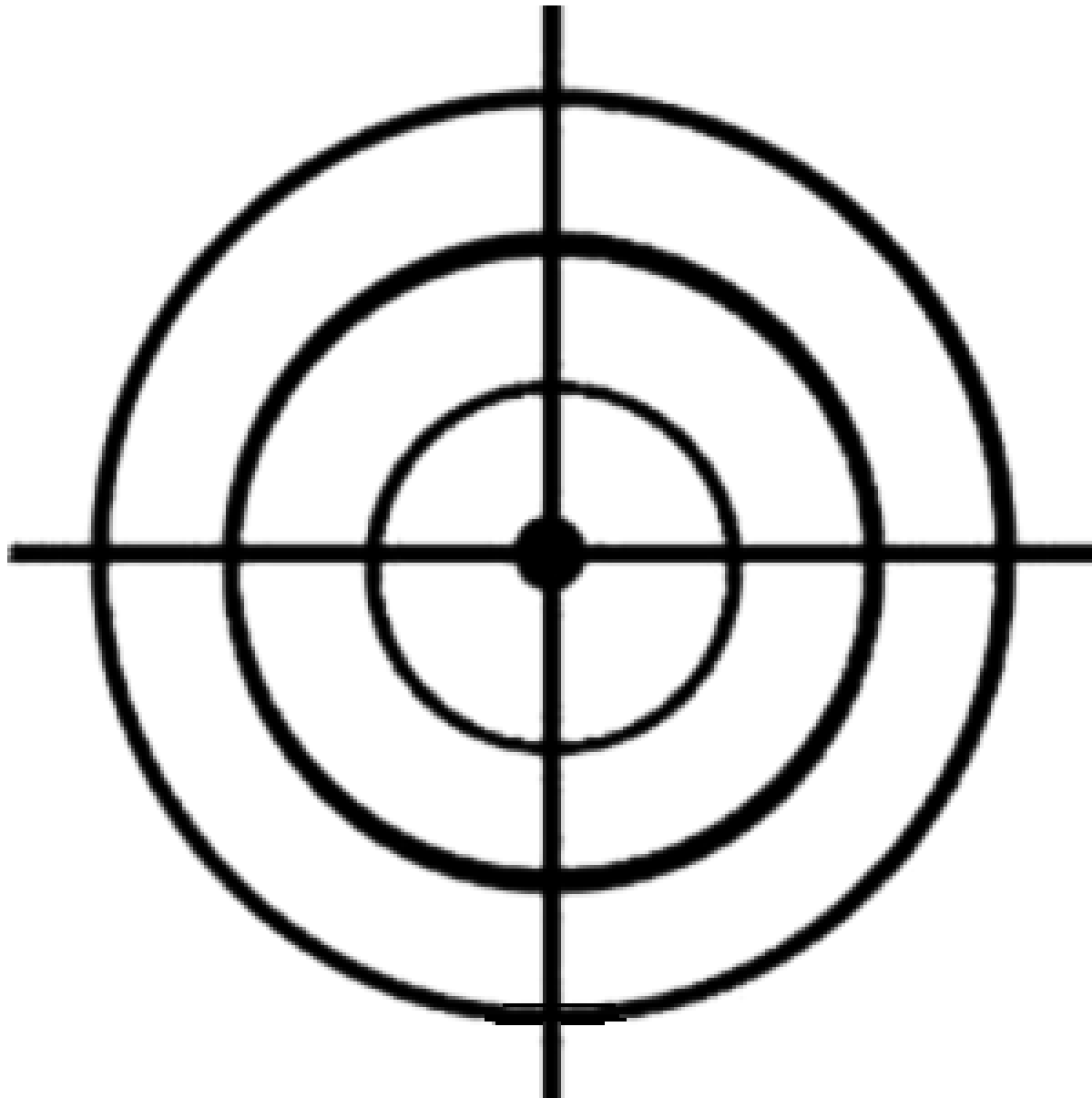
Quelle: Internet Security Threat Report 2013

1 Daten und Fakten

2 Gezielte Angriffe

3 Gewöhnliche Angriffe

4 Maßnahmen



# Auch Angreifer haben sich entwickelt



Der einsame Hacker



Professionelle Angreifer

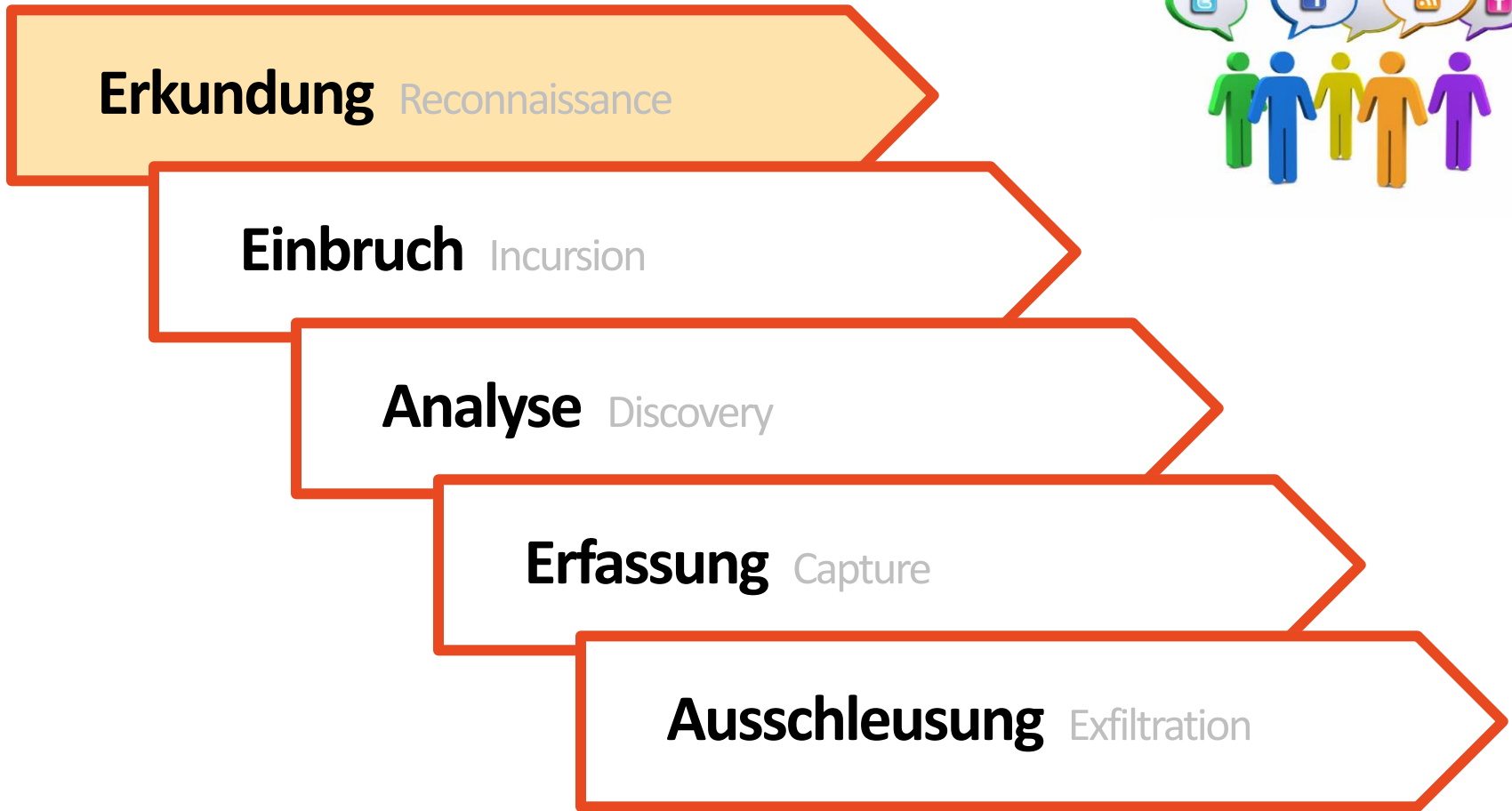


Der Anstieg bei  
gezielten Angriffen  
beträgt

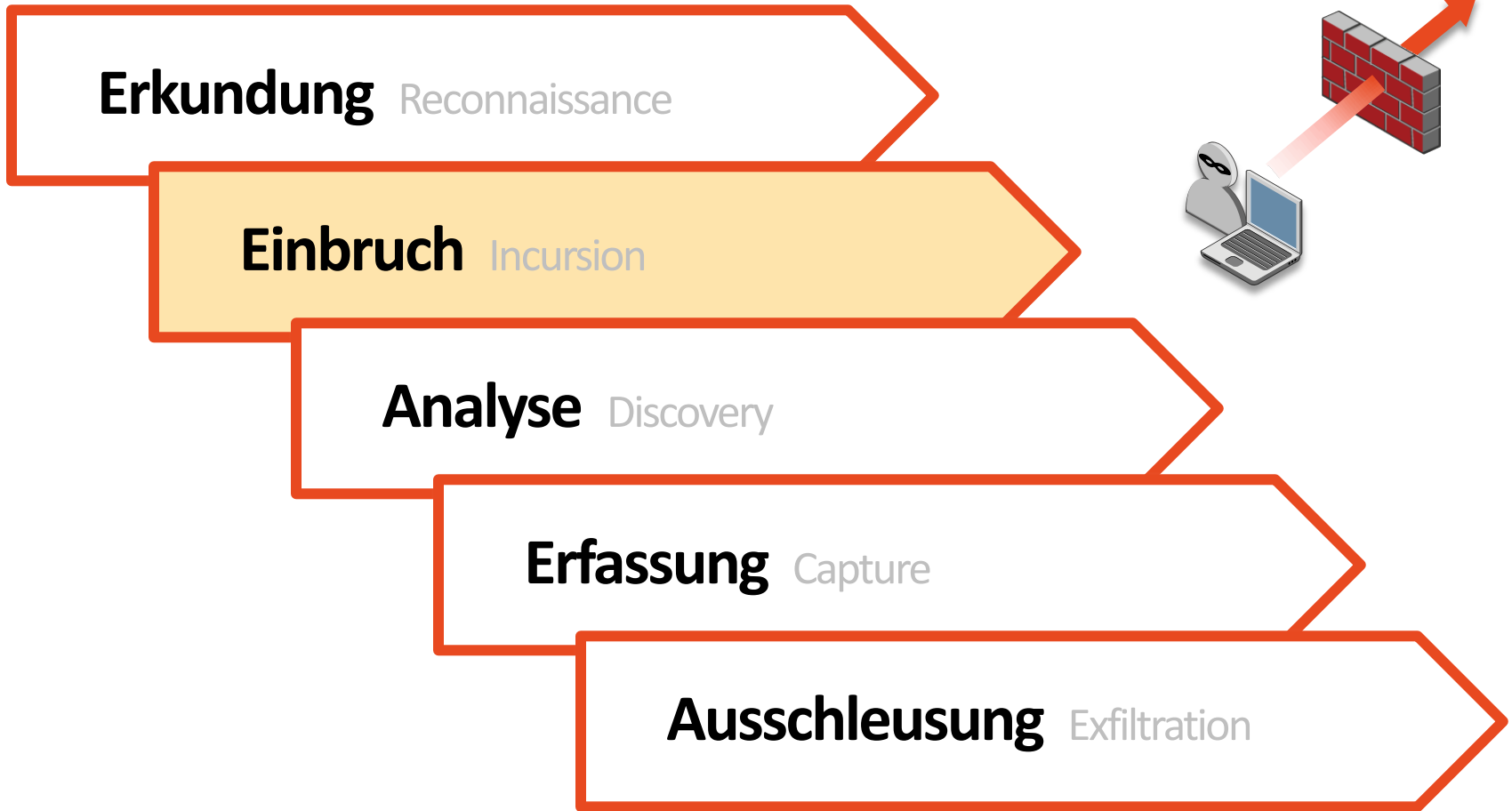
42%

in 2012

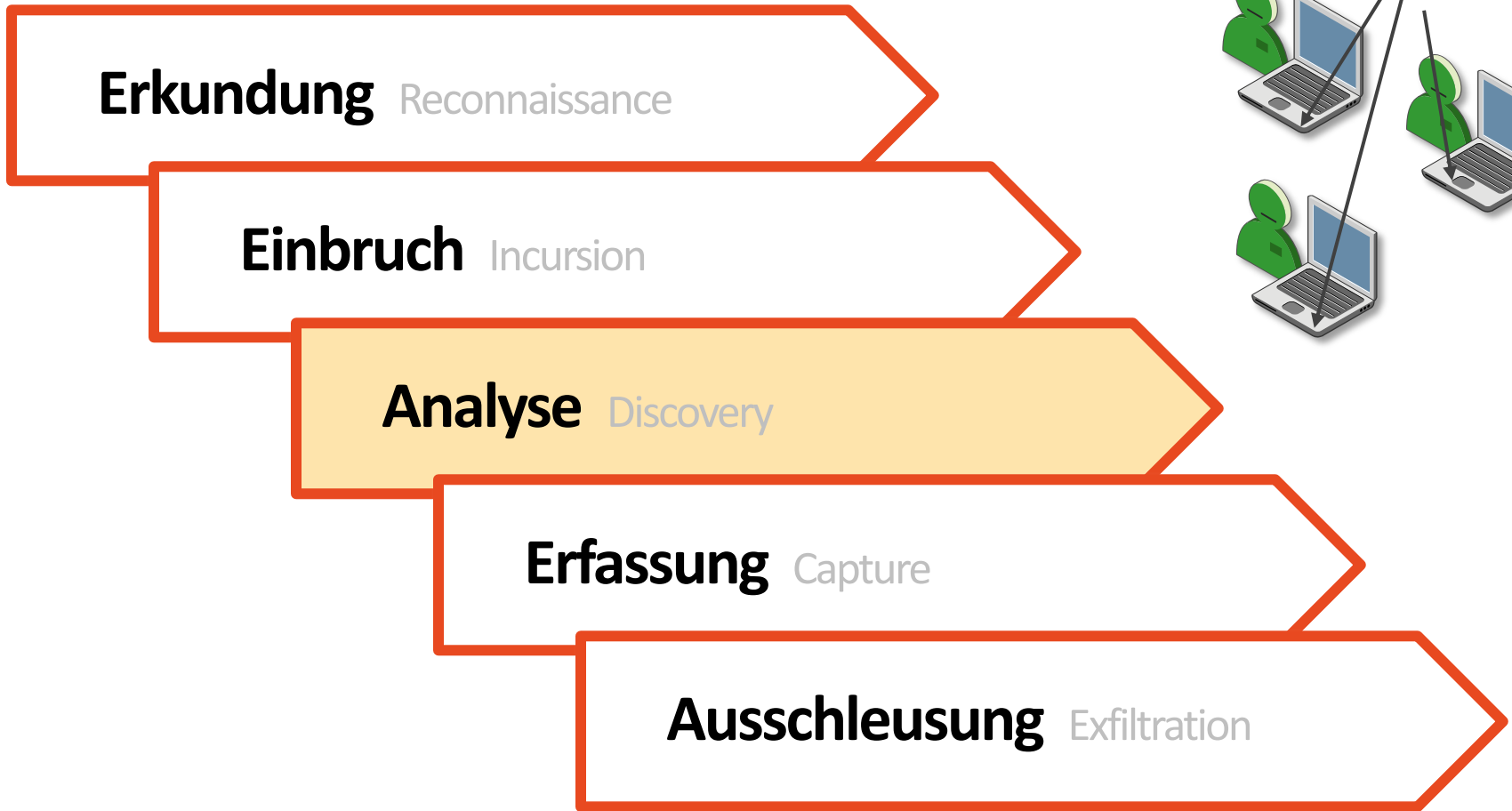
# Anatomie eines gezielten Angriffs



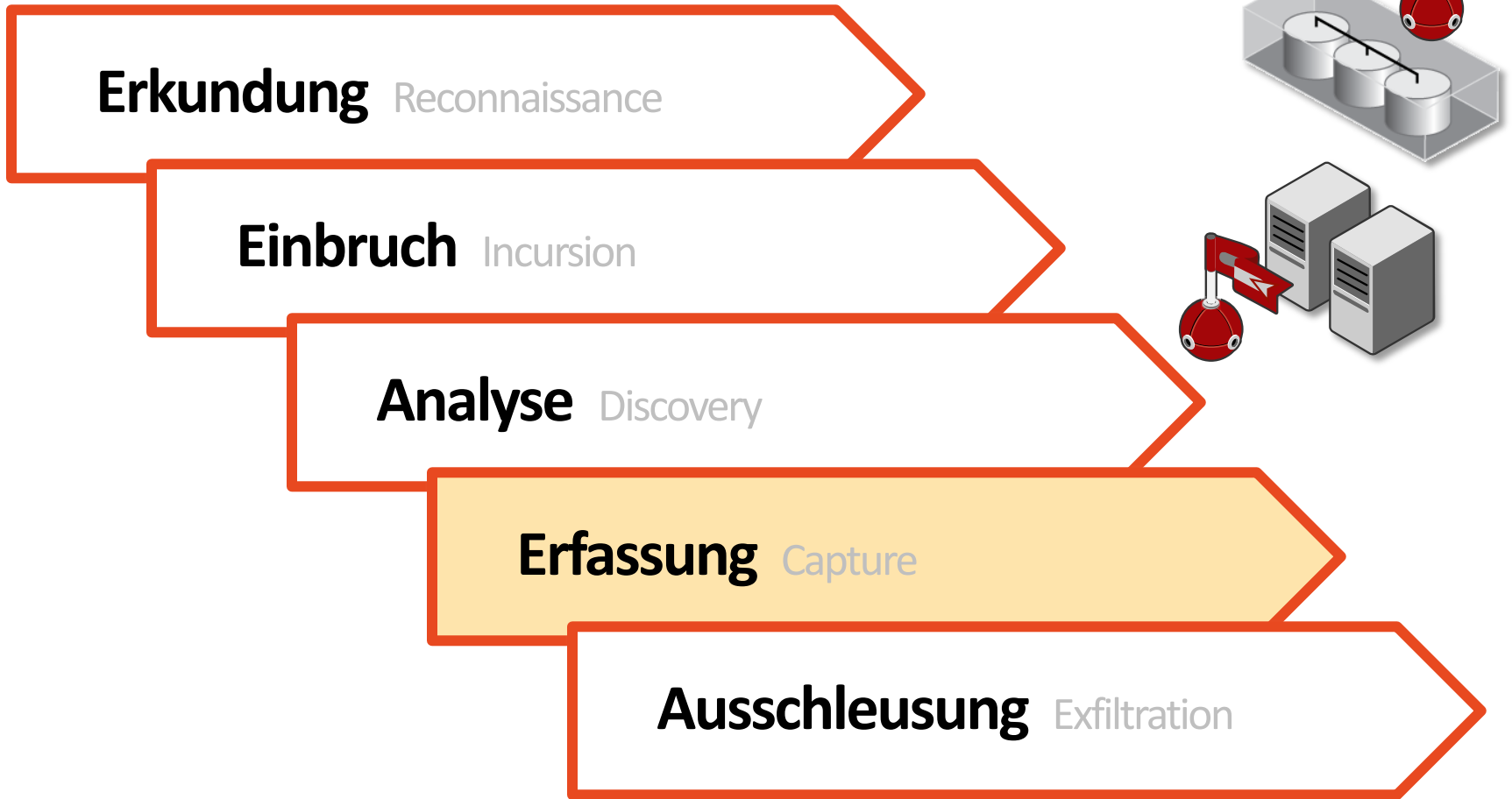
# Anatomie eines gezielten Angriffs



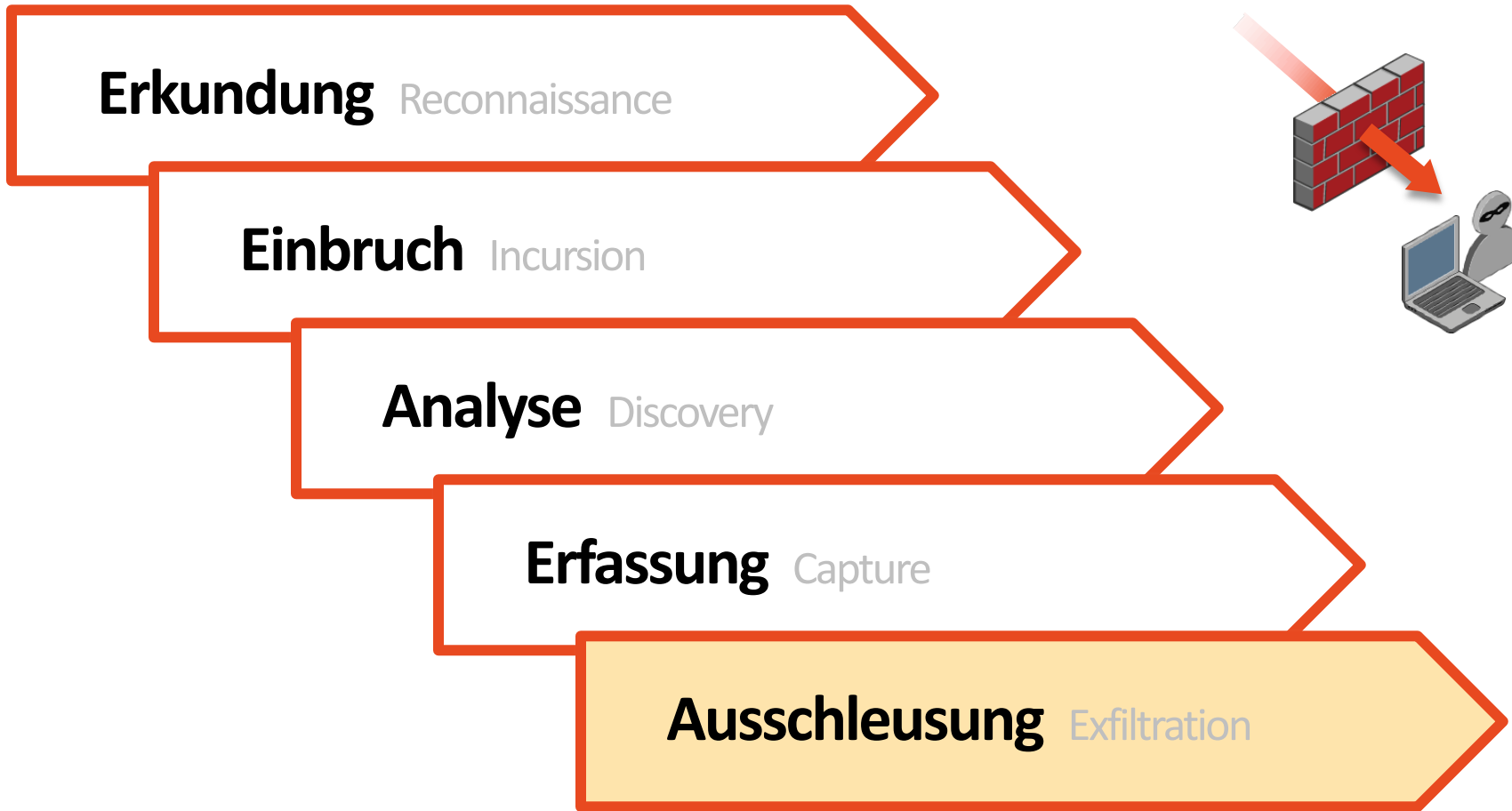
# Anatomie eines gezielten Angriffs



# Anatomie eines gezielten Angriffs



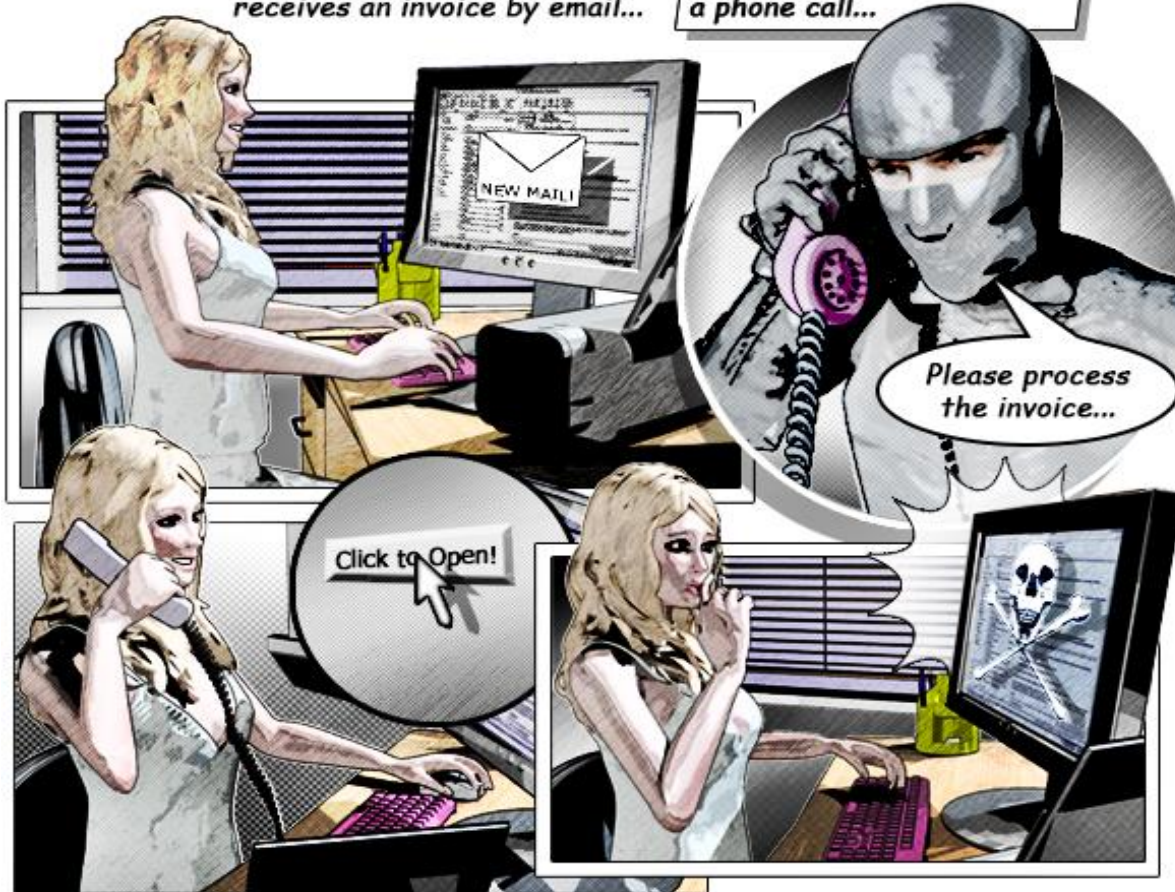
# Anatomie eines gezielten Angriffs



# Ein aktuelles Beispiel aus Europa

*An employee of a multinational company receives an invoice by email...*

*Minutes later, she receives a phone call...*



1 Daten und Fakten

2 Gezielte Angriffe

3 Gewöhnliche Angriffe

4 Maßnahmen





# Haben Sie diese Seiten in letzter Zeit besucht?



# Webseiten werden gegen uns verwendet

## Watering Hole Attack



Infektion einer  
legitimen Website

**53%**

der legitimen Webseiten  
haben Schwachstellen

**24%**

haben kritische  
Schwachstellen

**61%**

verseuchter Websites  
sind legitime Angebote

1 Daten und Fakten

2 Gezielte Angriffe

3 Gewöhnliche Angriffe

4 Maßnahmen



# Maßnahmen

- **Grundlagen** überprüfen
- **Richtlinien** erarbeiten
- **Mitarbeiter** sensibilisieren
- **Einhaltung** überprüfen
- **Partner** einbeziehen



## Acht Tipps, Daten besser zu schützen

**Passwörter** wie 12345 oder der eigene Geburtstag sind unsicher. Vor allem, wenn sie auf einem Post-It am PC kleben.

Nicht auf **unbekannte Links** oder Anhänge in E-Mails klicken – Sie verpassen keinen Freiflug, sondern einen Virus.

**Geschäftsdaten** nicht über unsichere File Share Services oder Social Media teilen, außer der Wettbewerb soll mitlesen.

Auch mobile Geräte wie Smartphones oder Tablets mit einem **Passwort schützen** – oder möchten Sie dem Dieb Ihres Handys Einsicht ins Unternehmen geben?

Vorsicht bei **Zugriffsberechtigungen**, wenn Sie Apps herunterladen – egal, wer im Hintergrund mitliest oder weiterleitet.

Vorsicht bei **dubiosen Freundschaftsanfragen** in sozialen Netzwerken – Cyber-Kriminelle sind keine guten Freunde.

Standardmäßig eine **Anti-Malware-Lösung** einsetzen und immer auf dem neuesten Stand halten, ansonsten öffnen Sie Hackern Tür und Tor.

Daten kontinuierlich **sichern**. Falls morgen der Server ausfällt, sind die Informationen schnell in der Cloud zugänglich.

Weitere Infos finden Sie  
in unserem Sicherheitsbericht.





# Binden Sie Partner ein !

The screenshot shows a web browser window with several tabs: Facebook, Amazon.de, Nachrichten und aktuelle I..., Symantec Network Connec..., and Business Marketplace - Fi... The address bar shows the URL https://apps.telekomcloud.com/home. The page header includes the Deutsche Telekom logo, the text 'Business Marketplace', and a login button 'Anmelden'. Below the header are navigation links for 'Shop', 'Informationen', and 'Hilfe', along with 'Registrieren' and 'English'. A search bar contains the text 'Shop durchsuchen'. On the left, a 'Kategorien' section lists: Finanzen & Buchhaltung, Kundenmanagement, Projektmanagement, Zusammenarbeit, Marketing & Web, Service & Support, and Sicherheit. The main content area features a large yellow advertisement for Symantec. The ad includes the Symantec logo, the text 'Automatische Backups & Virenschutz', and a headline: 'Datensicherheit muss nicht teuer sein, aber Daten zu verlieren, kann Sie alles kosten.' Below the headline are two bullet points: '40% aller Cyber-Angriffe richten sich gegen Unternehmen mit weniger als 500 Mitarbeiter.' and 'Das Risiko für KMUs durch Malware Angriffe ist viermal so hoch als für größere Unternehmen.' A pink box in the top right of the ad says '30 TAGE KOSTENLOS TESTEN!'. A pink button at the bottom right says 'Symantec kennenlernen'. Small footnotes at the bottom of the ad cite 'Symantec SMB Threat Awareness Poll, 2011' and 'Symantec.cloud Skeptic™ System Data'.