# Intelligent Cybersecurity for the Real World

Wolfram Schulze
wschulze@cisco.com

Januar 2015

# Inhalt dieser Präsentation:

- Aktuelle Bedrohungslage, Cisco Security Report: Dem Sicherheitsteam von Cisco zufolge war in 100 Prozent der untersuchten Netzwerke schädlicher Datenverkehr nachweisbar
- Cisco Security Strategie: Ende-zu-Ende Security, Korrelation von relevanten Daten, Reduzierung der Komplexität
- Herkömmliche NGFWs reichen nicht aus, sie sind nur auf Anwendungen ausgerichtet, Bedrohungen mit anderem Gefahrenpotenzial werden ignoriert

How would you do security differently if you knew you were going to be hacked?

TECHNIK

Viele Menschen bewegen sich zu sorglos im Internet.
(Foto: picture alliance / dpa)

Dienstag, 13. Januar 2015

## BSI beklagt digitale Sorglosigkeit

# Eine Million deutsche Computer infiziert

**Viele Menschen unterschätzen die Gefahr durch Cyberkriminalität und vernachlässigen den Schutz ihrer Computer. Mehr als eine Million Rechner sind in Deutschland infiziert und die meisten ihrer Nutzer wissen es nicht mal. Warum ist das so?**

Die oberste Behörde für die IT-Sicherheit in Deutschland warnt vor wachsenden Bedrohungen im Internet und beklagt eine "digitale Sorglosigkeit" vieler Bürger und Firmen. "Die Angreiferszene rüstet auf", sagt der Präsident des Bundesamts für Sicherheit in der

Laut Hange sind mehr als eine Million Rechner in Deutschland mit Schadprogrammen infiziert und in sogenannten Botnetzen zusammengeschlossen, mit denen die Computer für Cyberangriffe ferngesteuert werden können. "Das ist ein erhebliches Gefahrenpotenzial." Jeder Rechner könne zu einem Tatwerkzeug werden, ohne dass der Nutzer das überhaupt merke.

### Viele Firmen knauserig

Cyberangriffe seien bequem und das Entdeckungsrisiko für die Täter gering, betonte der BSI-Chef. Die technischen Instrumente seien im Netz zu kaufen und beispielsweise Botnetze zu mieten. Das Dunkelfeld der Cyberkriminalität sei sehr groß und die Aufklärungsquote niedrig. Die Sensibilität für die Gefahren im Cyberraum bei Bürgern und Firmen habe sich durch die Snowden-Enthüllungen die millionenfachen Diebstähle von Online-Identitäten Anfang 2014 sowie die wiederkehrenden Meldungen über gestohlene Kundendaten in Unternehmen hätten dazu geführt, dass die Aufmerksamkeit für das Thema IT-Sicherheit angestiegen und gleichzeitig das Vertrauen in die IT erschüttert ist, heißt es im BSI-Bericht. Eine "digitale Sorglosigkeit" sei aber noch immer weit verbreitet, sagt Hange: "Viele Nutzer und Firmen merken gar nicht, wenn sie Opfer einer Cyberattacke werden." Zum Teil fehle es an Kompetenz, Gefahren zu erkennen und für genügend Schutz zu sorgen. In vielen Firmen werde außerdem zu wenig in IT-Sicherheit investiert. Gerade bei kleinen mittelständischen Firmen hapere es noch.

MEHR ZUM THEMA

12.01.15
Microsoft muss viele Lücken stopfen
**Internet Explorer ist Hackers Liebling**

12.01.15
Hacker kapern Router für Botnetz
**Ist die Fritzbox sicher?**

09.01.15
Andere surfen viel schneller
**Deutschland bleibt Internet-Schnecke**

Das BSI hat im Lagebericht vier Maßnahmenbereiche definiert, die von der Förderung der Kompetenz und Vertrauenswürdigkeit im Bereich IT-Sicherheit über ein verstärktes Engagement bei Zertifizierung und Standardisierung sowie der Förderung der breitflächigen Anwendung sicherer Technologien bis hin zum verstärkten Schutz Kritischer Infrastrukturen reichen. Konkrete Hilfen oder Anleitungen finden sich dort allerdings nicht. Das BSI betont die Eigenverantwortung der Nutzer, will aber den Einsatz "sicherer und vertrauenswürdiger Technologien" fördern. Von "entscheidender Bedeutung" sei dabei "die Entwicklung, Bereitstellung und durchgängige Anwendung vertrauenswürdiger Krypto- und Cyber-Technologien für alle Zielgruppen. Handfestere Tipps finden Nutzer im "Leitfaden für Informationssicherheit" des BSI.

n-tv

Suchen auf n-tv.de

Home | Politik | Wirtschaft | Börse | Sport | Panorama | Unterhaltung | Technik | Ratgeber

Startseite » Technik » Da lachen sich Hacker kaputt : Hitliste der 25 blödesten Passwörter

TECHNIK

"Angry Kid" verkörpert den dummen Rüppel in den Abenteuern von "Wallace und Gromit". (Foto: Reuters)

Dienstag, 20. Januar 2015

## Da lachen sich Hacker kaputt

**Eine US-Firma veröffentlicht jährlich die am häufigsten geknackten Passwörter. Viel hat sich 2014 im Vergleich zum Vorjahr nicht geändert. Es gibt aber einen neuen Drittplatzierten und Sicherheits-Dummies stehen offenbar vermehrt auf Superhelden.**

Man ahnt es schon: Auch 2014 war "123456" das Passwort, das SplashData am häufigsten auf Listen mit geknackten Internet-Zugangsdaten gefunden hat. Zwar wertet das Sicherheitsunternehmen vor allem englische Dummie-Passwörter aus, aber zumindest die Spitzenpositionen dürften auch in Deutschland ganz vorne stehen.

Platz 1 der Hitliste der blödesten Passwörter belegt wie im Vorjahr "123456", gefolgt von dem Klassiker "password", der 2012 noch die Nummer 1 war. "12345" startete im vergangenen Jahr richtig durch, stürmte vom 20. Rang aufs Treppchen und verdrängte "12345678" vom dritten Platz. "qwerty" rutscht ebenfalls um einen Platz nach unten und ist jetzt Fünftplatzierter. "123456789", das 2013 bester Neueinsteiger war, verpasst als unverändert Sechster den Sprung in die Top 5. Neu in der Hitliste der blödesten Passwörter sind "superman" auf Platz 21 und "batman", der an 24. Stelle liegt.

Hier die von "Time" veröffentlichte komplette Liste:

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey

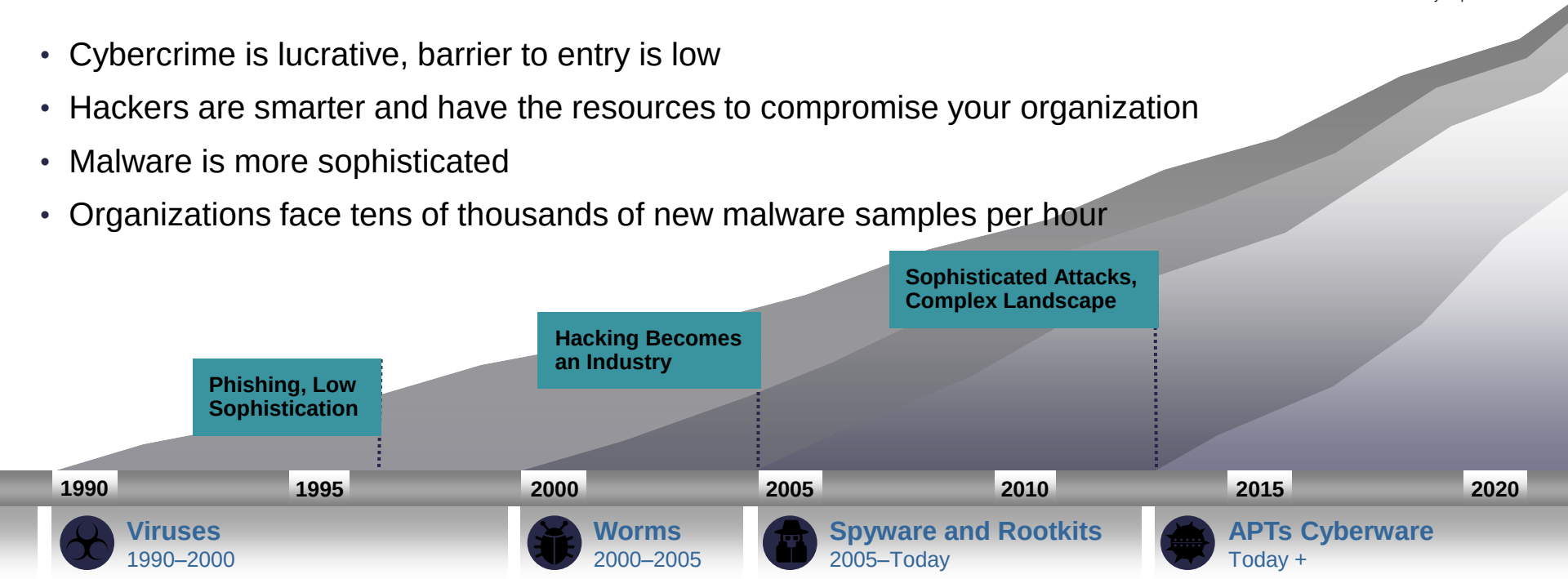
# The Reality: Organizations Are Under Attack

**95%** of large companies targeted by malicious traffic

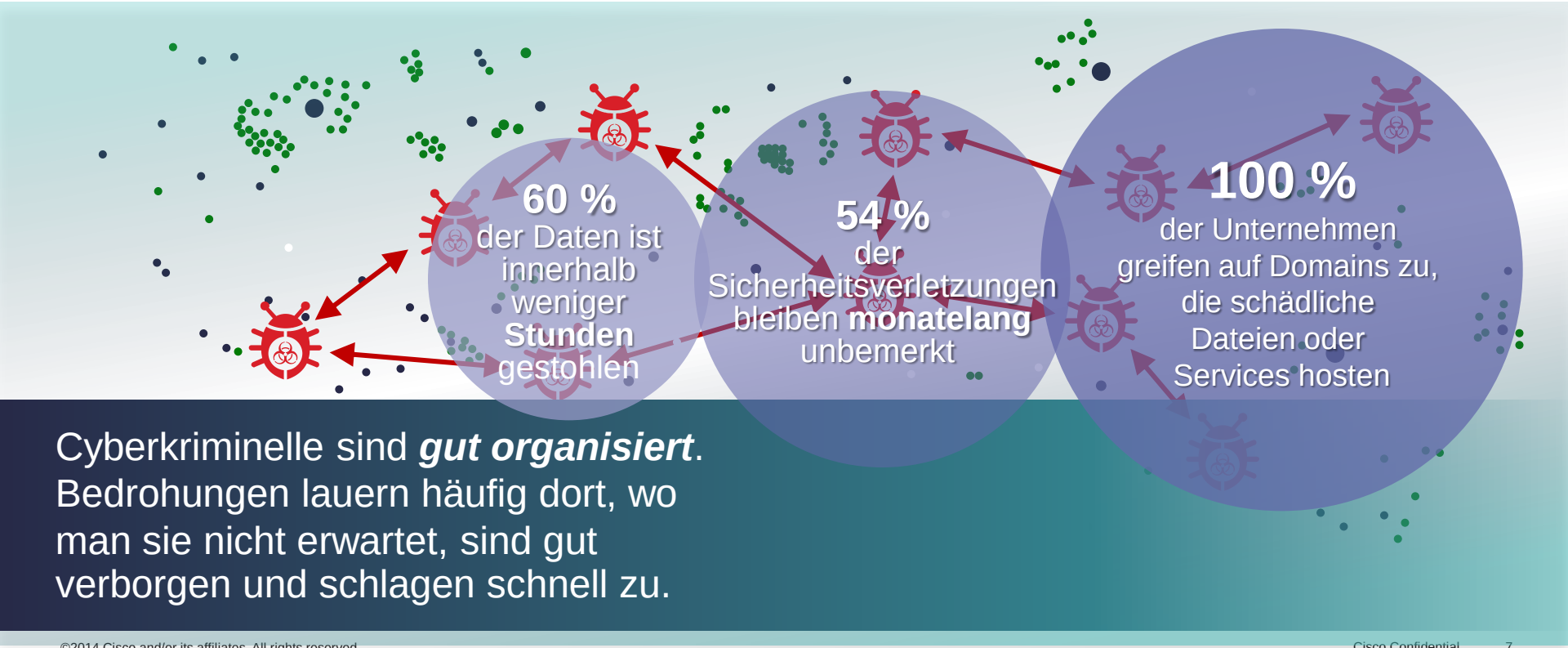
**100%** of organizations interacted with websites hosting malware

Source: 2014 Cisco Annual Security Report

- Cybercrime is lucrative, barrier to entry is low
- Hackers are smarter and have the resources to compromise your organization
- Malware is more sophisticated
- Organizations face tens of thousands of new malware samples per hour



# Heutige Bedrohungslandschaft erfordert mehr als nur Anwendungskontrolle




Cyberkriminelle sind ***gut organisiert***. Bedrohungen lauern häufig dort, wo man sie nicht erwartet, sind gut verborgen und schlagen schnell zu.

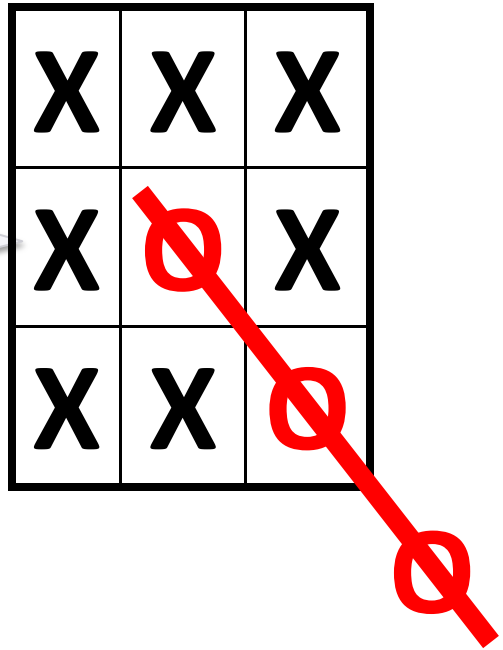
# Das Problem:
# **Advanced Malware**

Keine isolierten Programme - sondern **Ecosystems**

So kommt es immer wieder zu neuen Infizierungen!

# Thinking Beyond the Perimeter

Advanced Persistent Threats and other Modern threats are consistently bypassing the security perimeter as they ‘break the rules’.



Work, Your Way, *Securely*.

- Aktuelle Bedrohungslage
- **Intelligent Cybersecurity - Cisco’s Integrated Security Solution**
- Vorteile/Nachteile von NGWF Lösungen

# The Silver Bullet Does Not Exist

FW/VPN

"Block or Allow"

AV

"It matches the pattern"

PKI

"No key, no access"

IDS / IPS
UTM

"No false positives,
no false negatives."

NAC

"Captive portal"

Application
Control

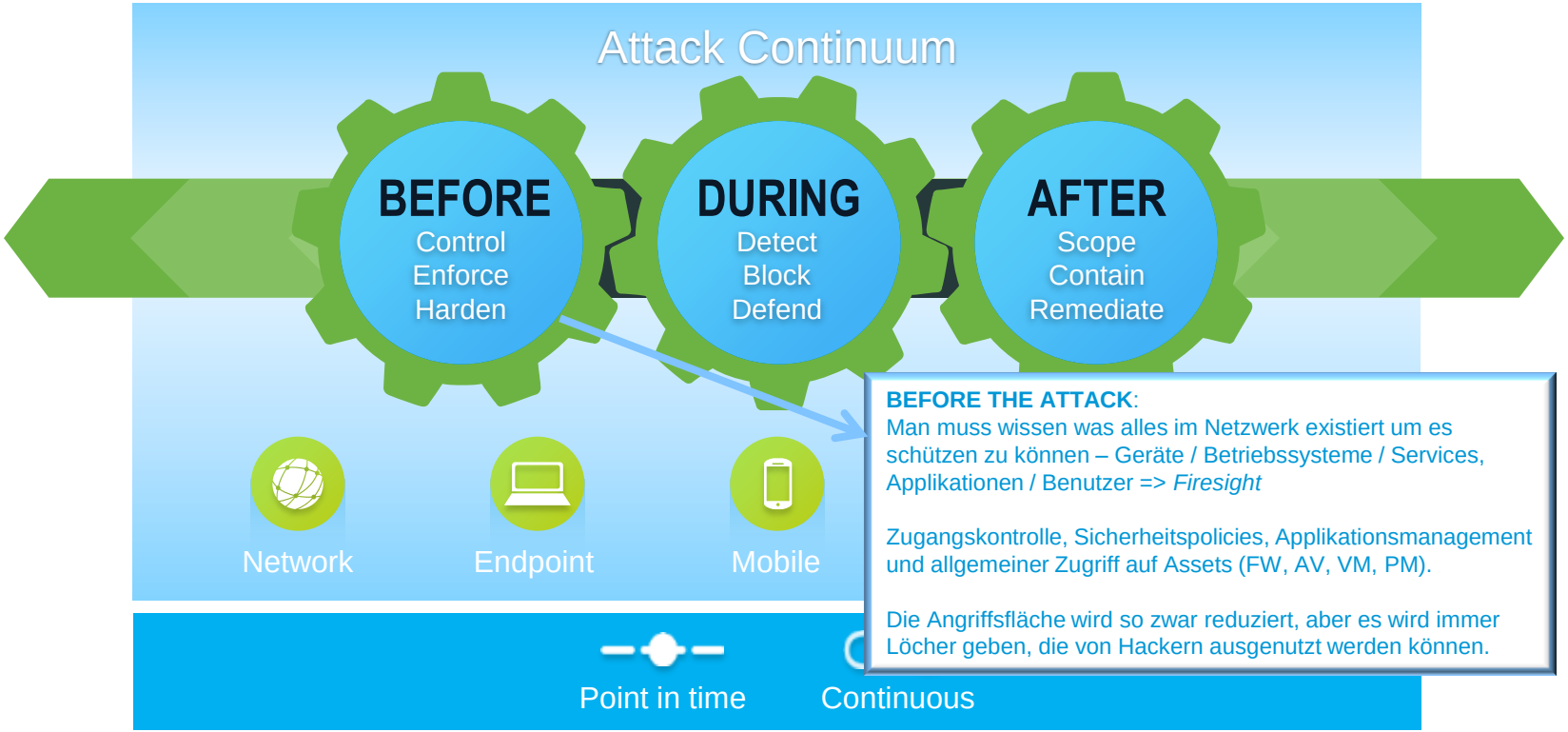
"Fix the Firewall"

Sandboxing

"Detect the
Unknown"

Cisco focuses on the totality of defending against threats

# The *Next Generation Security Model*

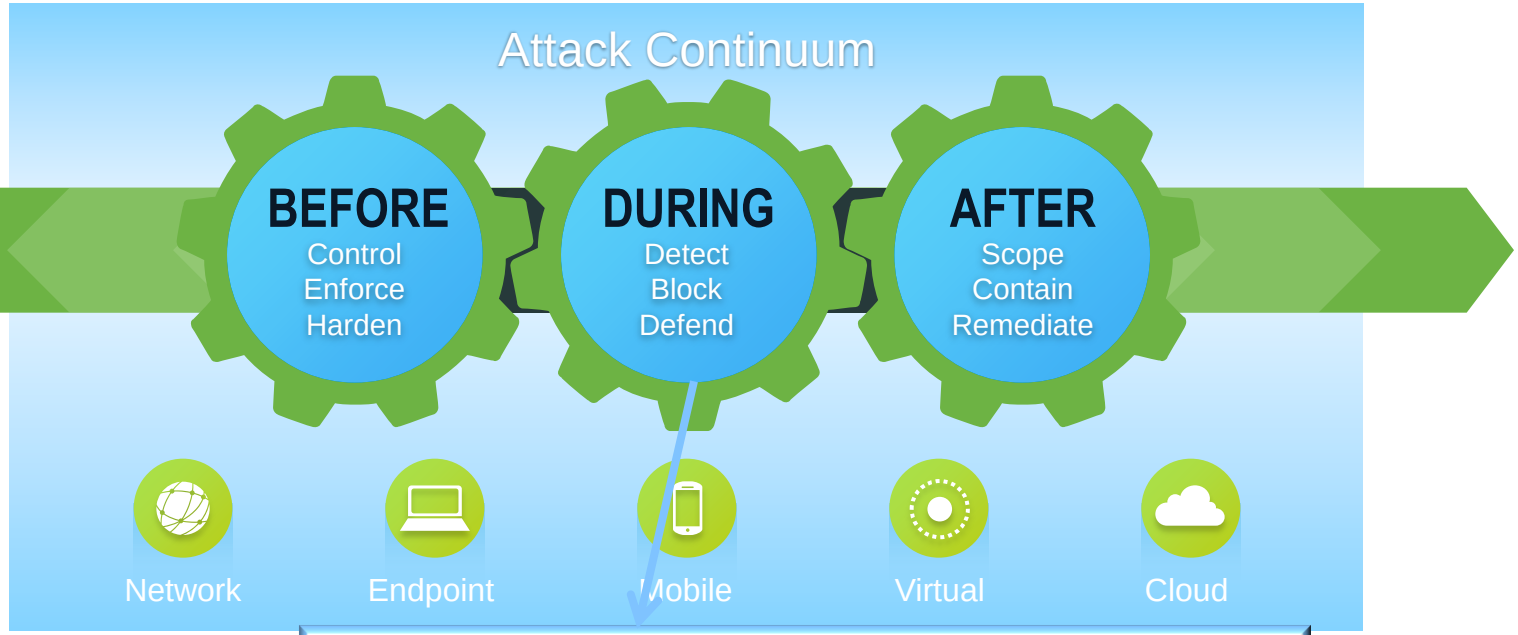



**BEFORE THE ATTACK**:
Man muss wissen was alles im Netzwerk existiert um es schützen zu können – Geräte / Betriebssysteme / Services, Applikationen / Benutzer => *Firesight*

Zugangskontrolle, Sicherheitspolicies, Applikationsmanagement und allgemeiner Zugriff auf Assets (FW, AV, VM, PM).

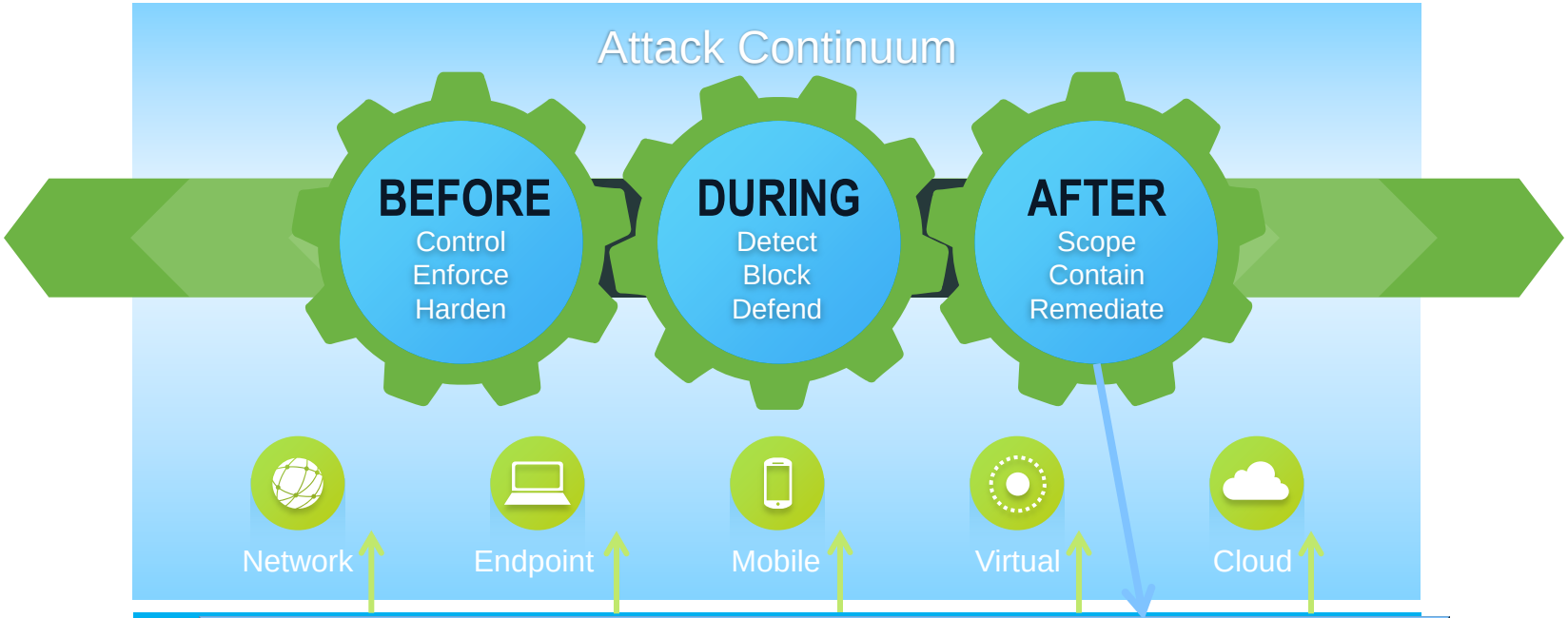
Die Angriffsfläche wird so zwar reduziert, aber es wird immer Löcher geben, die von Hackern ausgenutzt werden können.

# The *Next Generation Security Model*



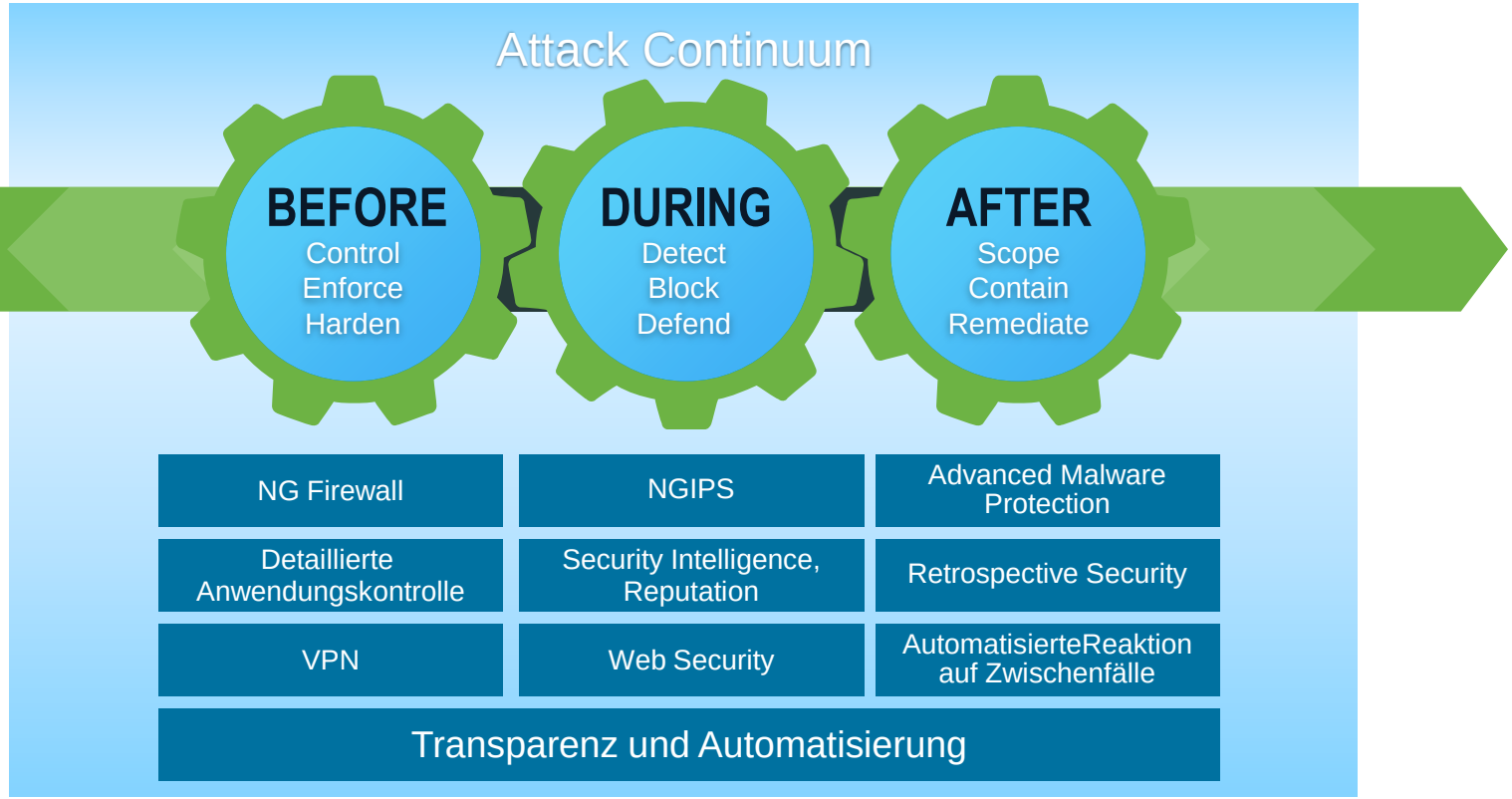

**DURING THE ATTACK**:
Die effizienteste Malware-Erkennungslösung ist notwendig (NG IPS). Diese Lösung muss multi-dimensional arbeiten und korrelieren können.
Sobald der Angriff erkannt wird, kann dieser geblockt werden und das Netzwerk dynamisch geschützt werden.

# The *Next Generation Security Model*




**AFTER THE ATTACK:**
Nichts desto trotz werden bestimmte Angriffe erfolgreich sein und das Unternehmen muss dann in der Lage sein, das Ausmass des Schadens zu bewerten, den Grund für das Event zu erkennen, einen Remediation Prozess zu starten und den eigentlichen Betrieb wieder zu normalisieren.
Die Lösung muss eine breite Palette and Angriffs-Vektoren adressieren können, da Malware sich überall manifestieren kann – im Netzwerk, am Client, auf Mobilen Geräten, in virtuellen Umgebungen, inklusive der Cloud.

# The *Next Generation Security Model*



Work, Your Way, *Securely*.

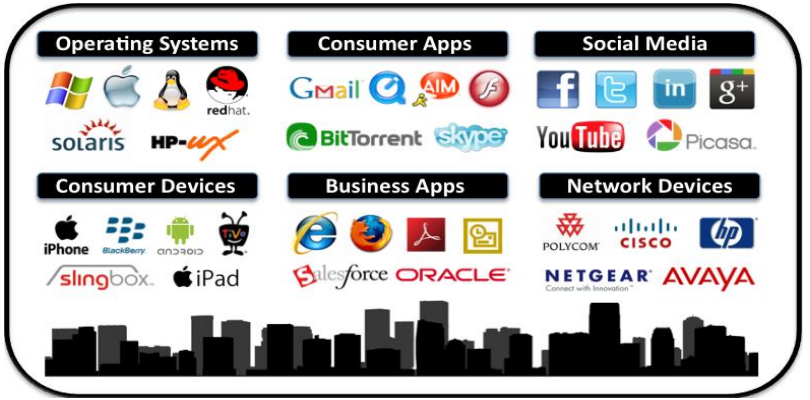
- Aktuelle Bedrohungslage
- Intelligent Cybersecurity - Cisco’s Integrated Security Solution
- **Vorteile/Nachteile von NGWF Lösungen**

# Neue Umstände erfordern neue Maßnahmen

NGFWs include the typical functions of traditional firewalls such as packet filtering,[2] network- and port-address Translation (NAT), stateful inspection, and virtual private network (VPN) support.[3] The goal of next generation firewalls is to include more layers of the OSI model to improve filtering of network traffic dependent on the packet contents

(Quelle: Wikipedia)

# (NG) Security Funktionen




- NGIPS
- AVC (App Control) / NGFW
- Advanced Malware Protection
- URL Filtering

- Clustering
- ACL
- VPN Termination
- NAT

Next Generation Services

Firewall

# Das Problem herkömmlicher Firewalls der nächsten Generation

## Fokus auf Anwendungen

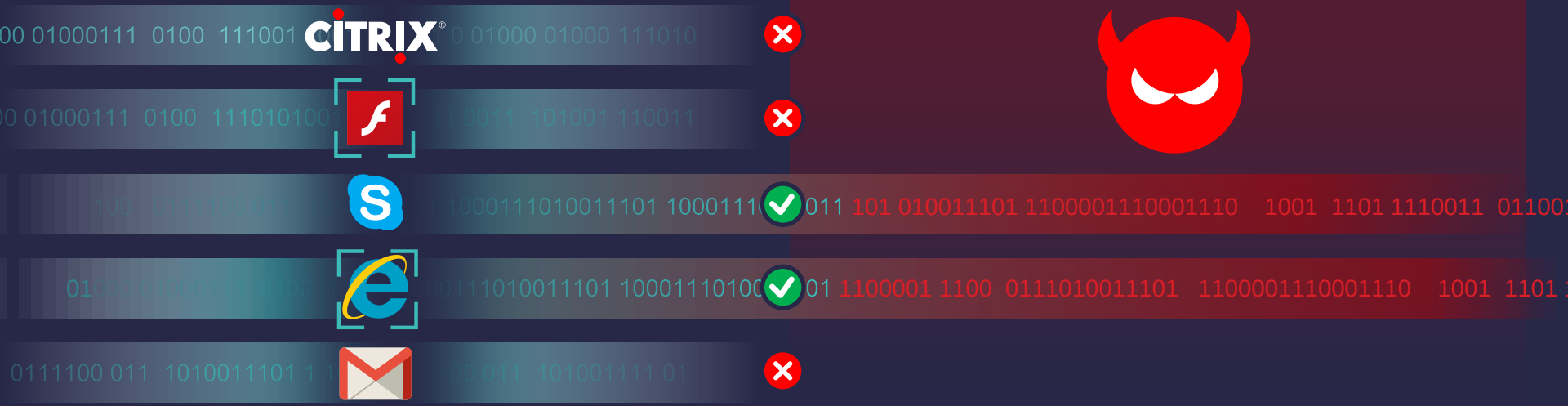

## Die Bedrohung wird außer Acht gelassen …

Herkömmliche NGFWs können die Angriffsfläche verkleinern, moderne Malware gelangt jedoch häufig durch die Sicherheitskontrollen.

# Das Problem herkömmlicher Firewalls der nächsten Generation

## Focus auf Anwendungen

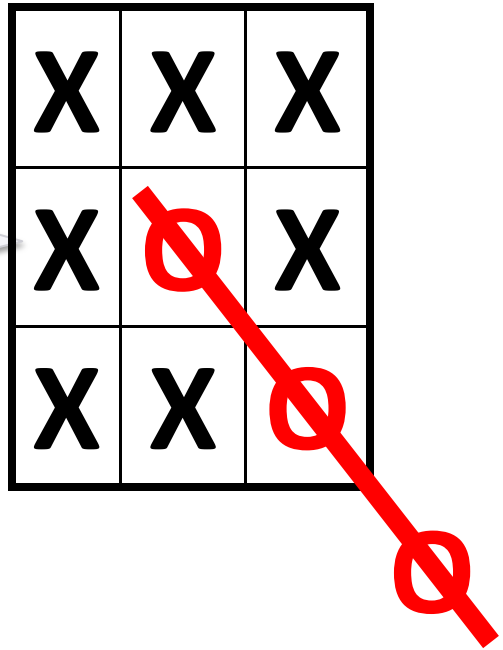
## …die Bedrohung wird außer Acht gelassen



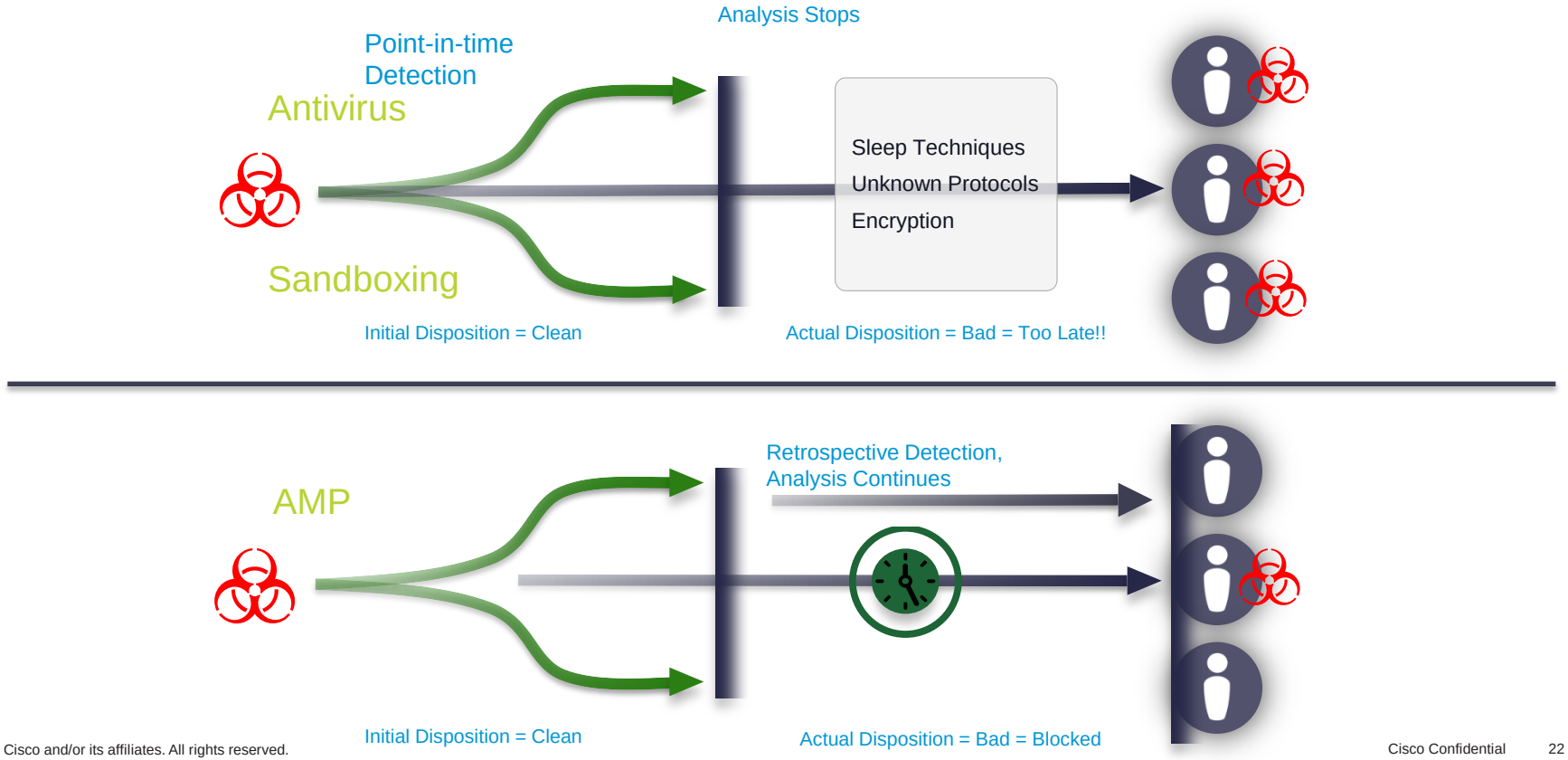

Herkömmliche NGFWs können die Angriffsfläche verkleinern, moderne Malware gelangt jedoch häufig durch die Sicherheitskontrollen.

# Thinking Beyond the Perimeter

Advanced Persistent Threats and other Modern threats are consistently bypassing the security perimeter as they ‘break the rules’.



# Continuous Protection when advanced malware evades point-in-time detection

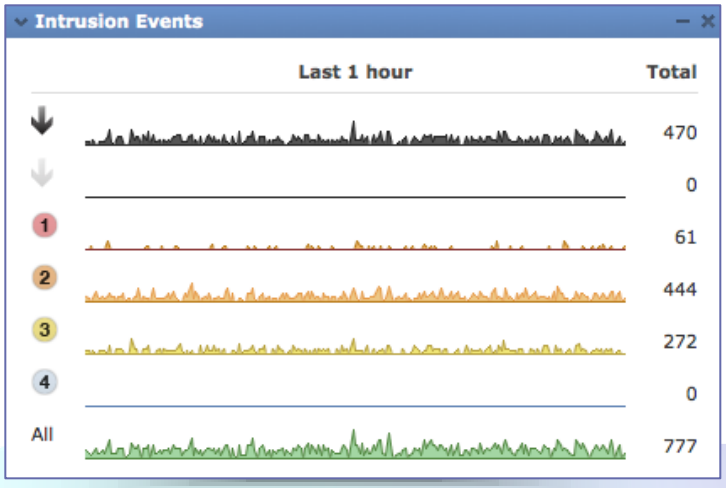


# Threat-Focused Next-Generation Firewall

# New Adaptive, Threat-Focused Next-Generation Firewall


## Cisco ASA

# Analyse der Auswirkungen




Korreliert alle Zugriffsversuchs-Ereignisse mit Auswirkungen auf das Ziel

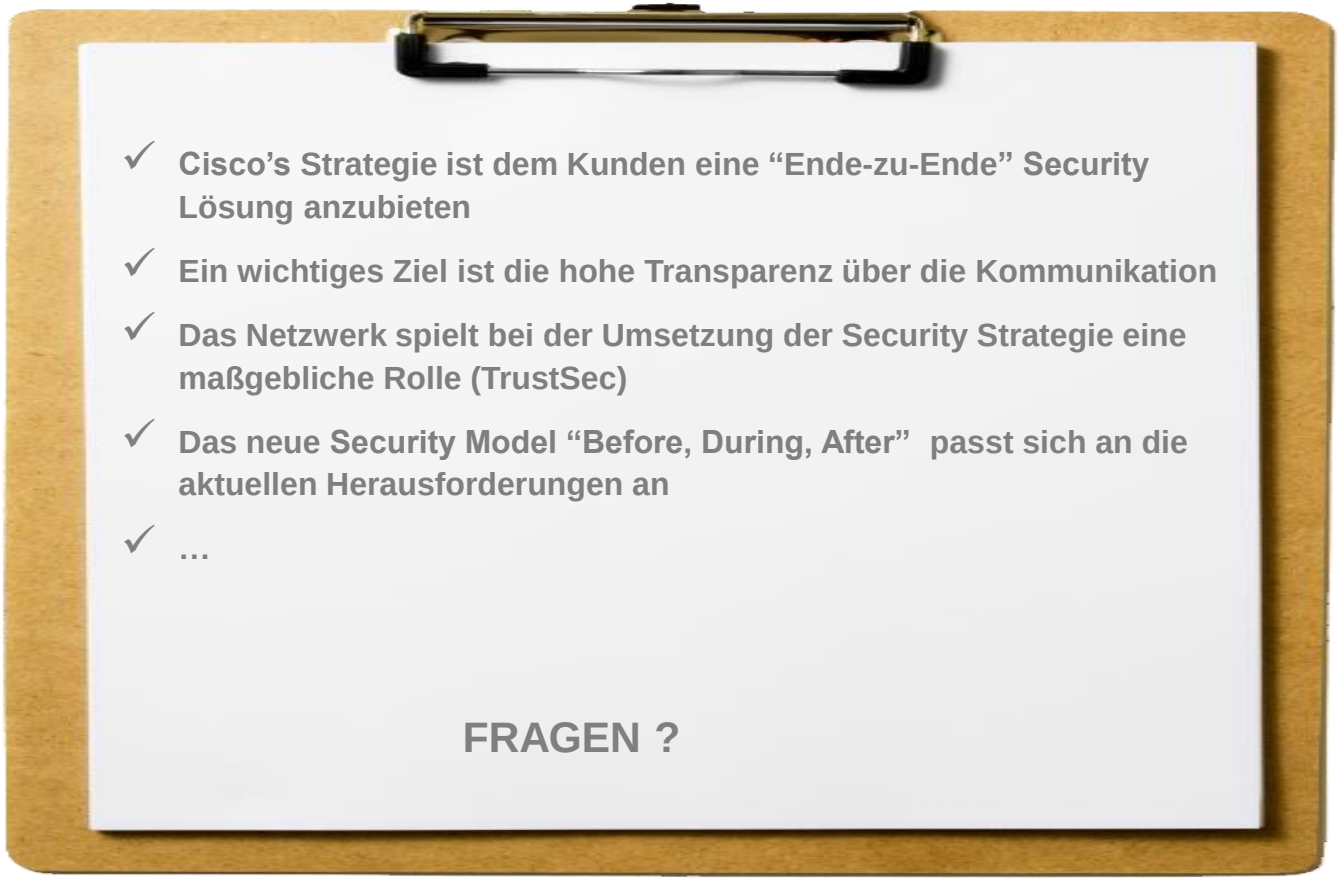
| IMPACT FLAG | MASSNAHMEN DES ADMINISTRATORS | GRUND |
|---|---|---|
| 1 | Sofortige Maßnahmen; Angreifbar | Ereignis deckt sich mit dem Host zugeordneten Schwachstellen |
| 2 | Untersuchen; Potentiell angreifbar | Entsprechender Port offen oder Protokoll in Verwendung, aber keine Schwachstelle erkannt |
| 3 | Wissenswert; Derzeit nicht angreifbar | Entsprechender Port nicht offen oder Protokoll nicht in Verwendung |
| 4 | Wissenswert; Ziel unbekannt | Überwachtes Netzwerk, aber Host unbekannt |
| 0 | Wissenswert; Netzwerk unbekannt | Nicht überwachtes Netzwerk |

# Security Report 2014


## Paradigmenwechsel bei Kompromittierungen: Ein Blick von innen nach außen


http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html

# Zusammenfassung



- ✓ **Cisco’s Strategie ist dem Kunden eine “Ende-zu-Ende” Security Lösung anzubieten**
- ✓ **Ein wichtiges Ziel ist die hohe Transparenz über die Kommunikation**
- ✓ **Das Netzwerk spielt bei der Umsetzung der Security Strategie eine maßgebliche Rolle (TrustSec)**
- ✓ **Das neue Security Model “Before, During, After” passt sich an die aktuellen Herausforderungen an**
- ✓ **…**

**FRAGEN ?**

Thank you.