25 Jahre WEISSBUCH

QuoVadis Sicherheit: Die Türen sind weit offen

Sonja Meindl, Country Manager Alps

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Sicherheitsbericht 2014

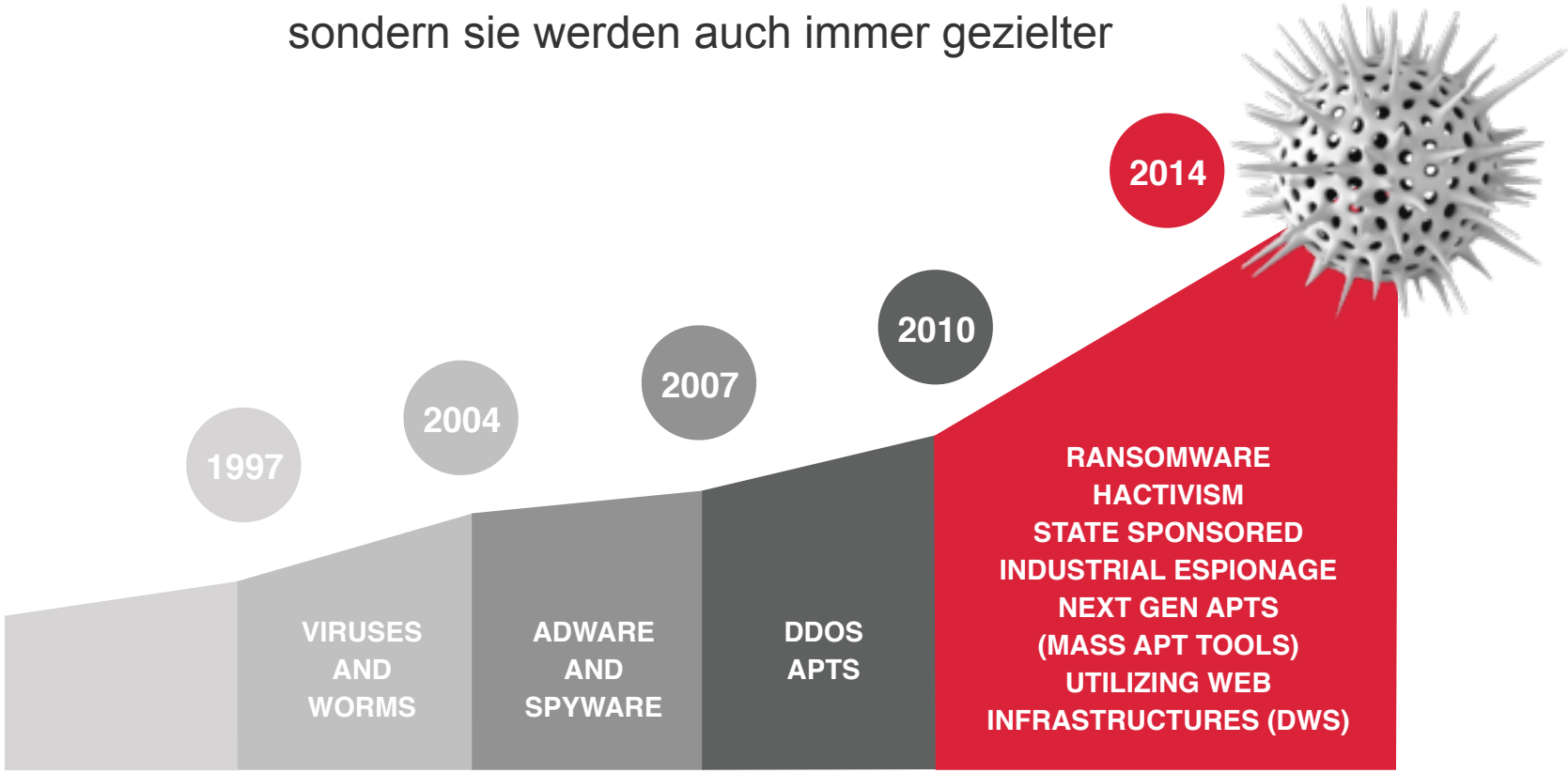
- Gateway-Eventdaten von **9‘240 Unternehmen**
- Ursachenanalyse von **Schadsoftware, Anwendungen und DLP Vorfällen**
- Zusammenfassung der Analysen des **Jahres 2013** in einem Bericht

Check Point *2014 Security Report*
Die wichtigsten Ergebnisse -

1. Explosionsartiger Ausbruch unbekannter Schadsoftware in 2013
2. Erhöhte Anzahl an Malwareinfizierungen
3. Verstärkter Einsatz risikoreicher Anwendungen im Unternehmen
4. Zunehmender, branchenübergreifender Datenverlust; Dateityp unabhängig

Permanent ändernde
BEDROHUNGSLANDSCHAFT

Die Anzahl der **BEDROHUNGEN** steigen nicht nur rasant an
sondern sie werden auch immer gezielter



53

UNBEKANNTE Malware-Dateien überwinden TÄGLICH die Schranken zum Unternehmensnetzwerk

Neue unbekannte Schadsoftware ist oft über Tage wirksam

<10% der AV Systeme entdecken unbekannte “wildlisted” Schadsoftware

2-3 Tage benötigt die Mehrheit der AV Systeme, um unbekannte Viren zu entdecken nachdem sie in der “Wildlist” vermerkt wurden

84%

DER UNTERNEHMEN HABEN EINE INFIZIERTE DATEI GELADEN

Erhöhte Anzahl an Schadsoftware-Infektionen in 2013

- Rechnerzugriff auf infizierte WebSite = jede Minute
  - *In 2012, waren es alle 23 Minuten*

Erhöhte Anzahl an Schadsoftware-Infektionen in 2013

- Rechnerzugriff auf infizierte WebSite = jede Minute
  - *In 2012, waren es alle 23 Minuten*

- Schadsoftware-Download = alle 10 Minuten
  - In 58% der Unternehmen waren dies Downloads alle 2 Stunden und weniger

Erhöhte Anzahl an Schadsoftware-Infektionen in 2013

- Rechnerzugriff auf infizierte WebSite = jede Minute
  - *In 2012, waren es alle 23 Minuten*

- Schadsoftware-Download = alle 10 Minuten
  - In 58% der Unternehmen waren dies Downloads alle 2 Stunden und weniger

- Bei 49% der Unternehmen wurden botinfizierte Rechner gefunden

Erhöhte Anzahl an Schadsoftware-Infektionen in 2013

- Rechnerzugriff auf infizierte WebSite = jede Minute
  - *In 2012, waren es alle 23 Minuten*

- Schadsoftware-Download = alle 10 Minuten
  - In 58% der Unternehmen waren dies Downloads alle 2 Stunden und weniger

- Bei 49% der Unternehmen wurden botinfizierte Rechner gefunden

- Alle 3 Minuten versucht ein Bot mit seinem C&C Server zu kommunizieren

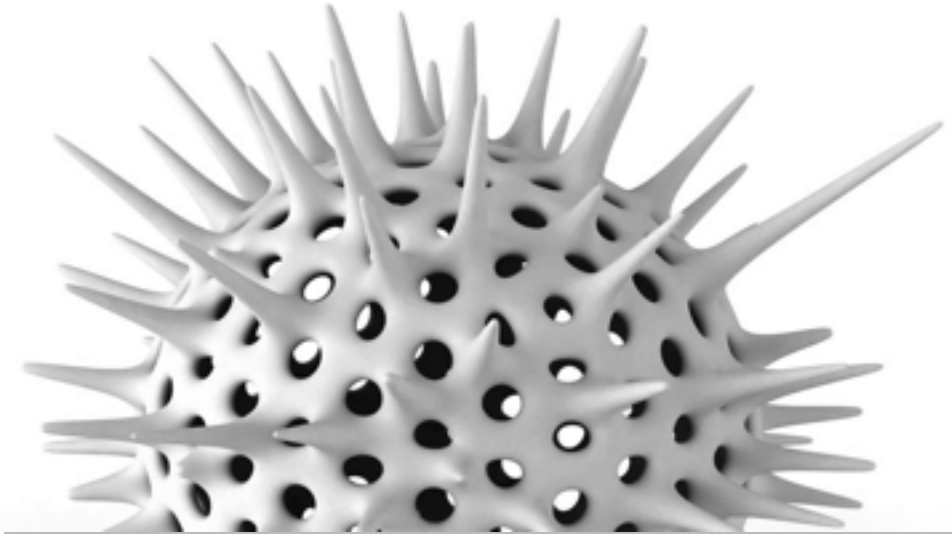
Bot-Infektionen in 2013
- verstärkt & fest verwurzelt -

77%

OF BOTS ARE ACTIVE FOR MORE THAN 4 WEEKS

77% MORE THAN 4 WEEKS

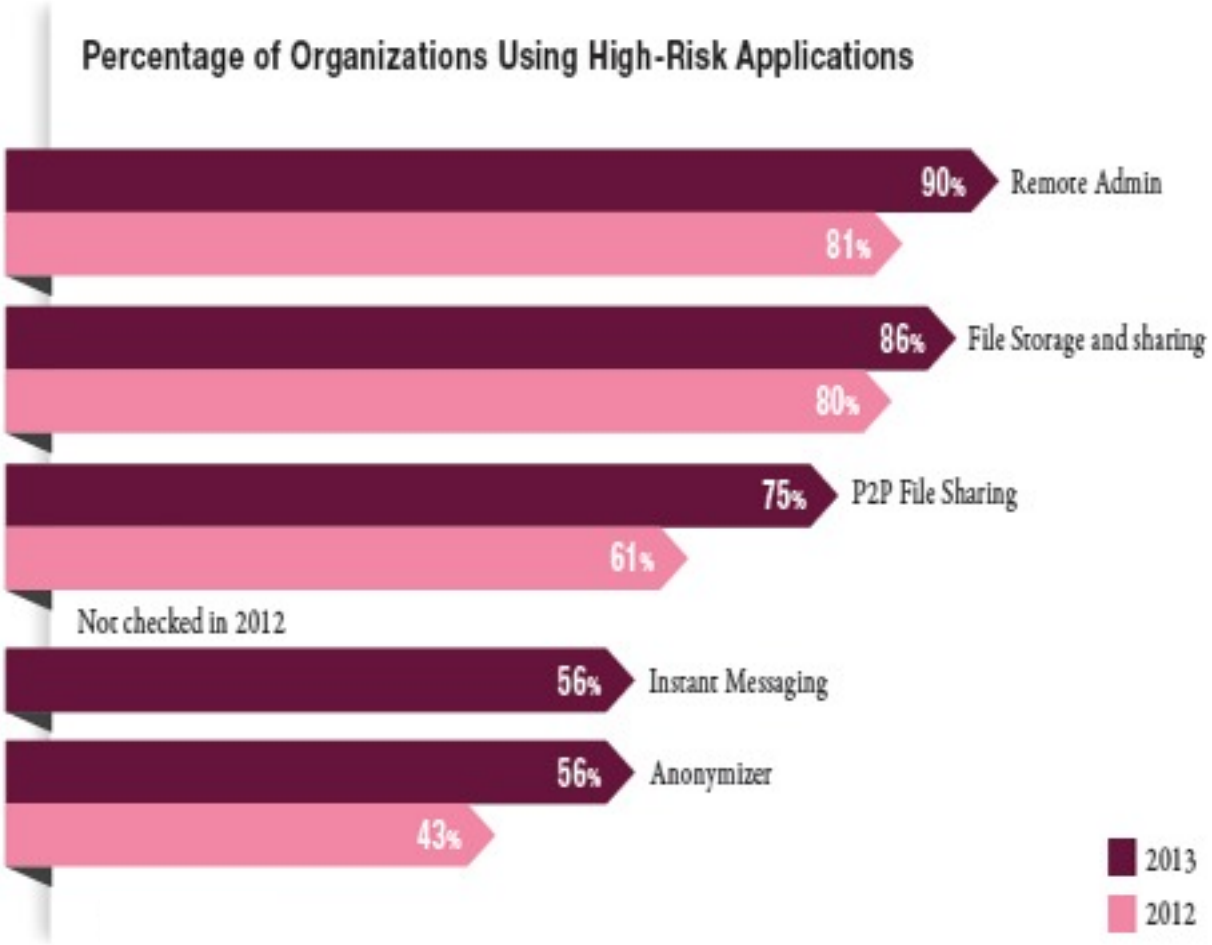
LESS THAN 4 WEEKS 23%



Check Point *2014 Security Report*
Die wichtigsten Ergebnisse -

1. Ausbruch unbekannter Schadsoftware in 2013
2. Erhöhte Anzahl an Malwareinfizierungen
3. Erhöhter Einsatz risikoreicher Anwendungen im Unternehmen
4. Zunehmender, branchenübergreifender Datenverlust; Dateityp unabhängig

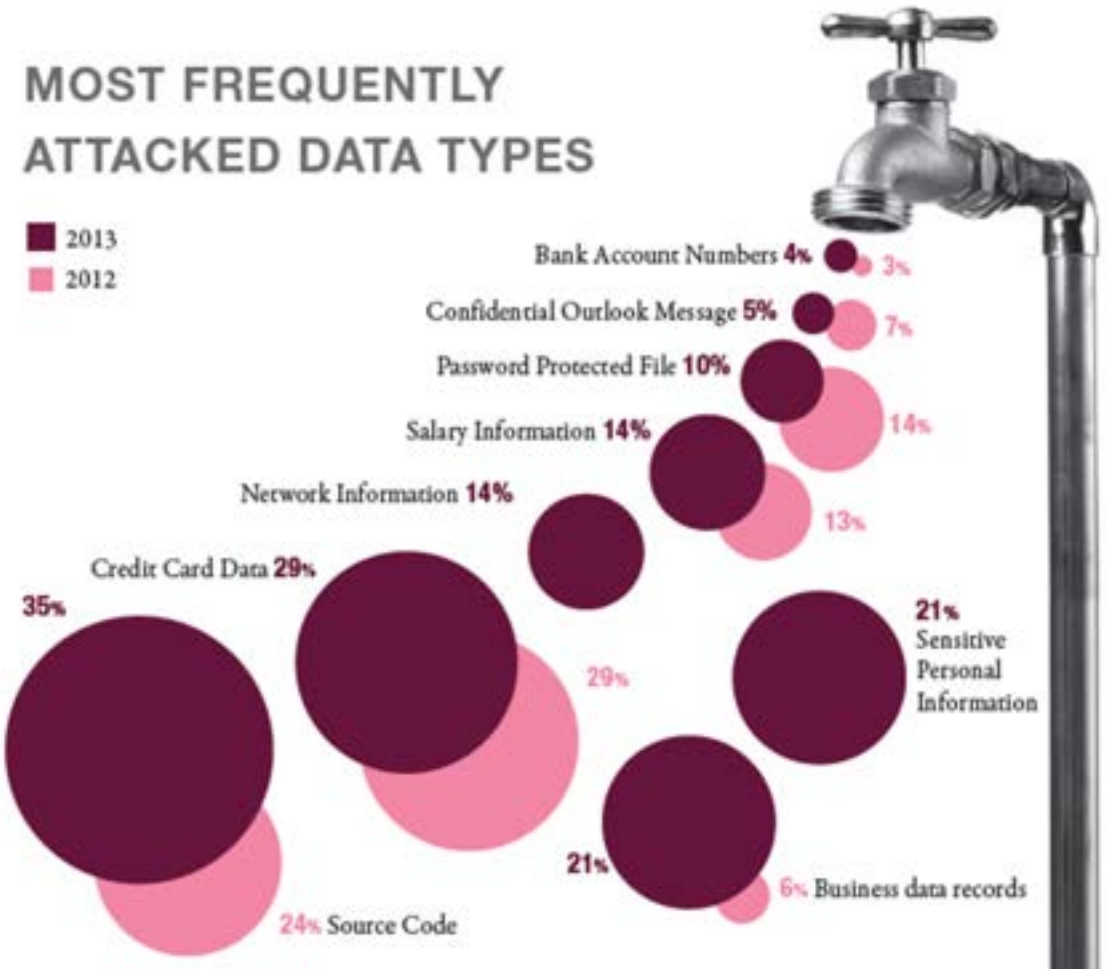
Verstärkter Einsatz risikoreicher Anwendungen



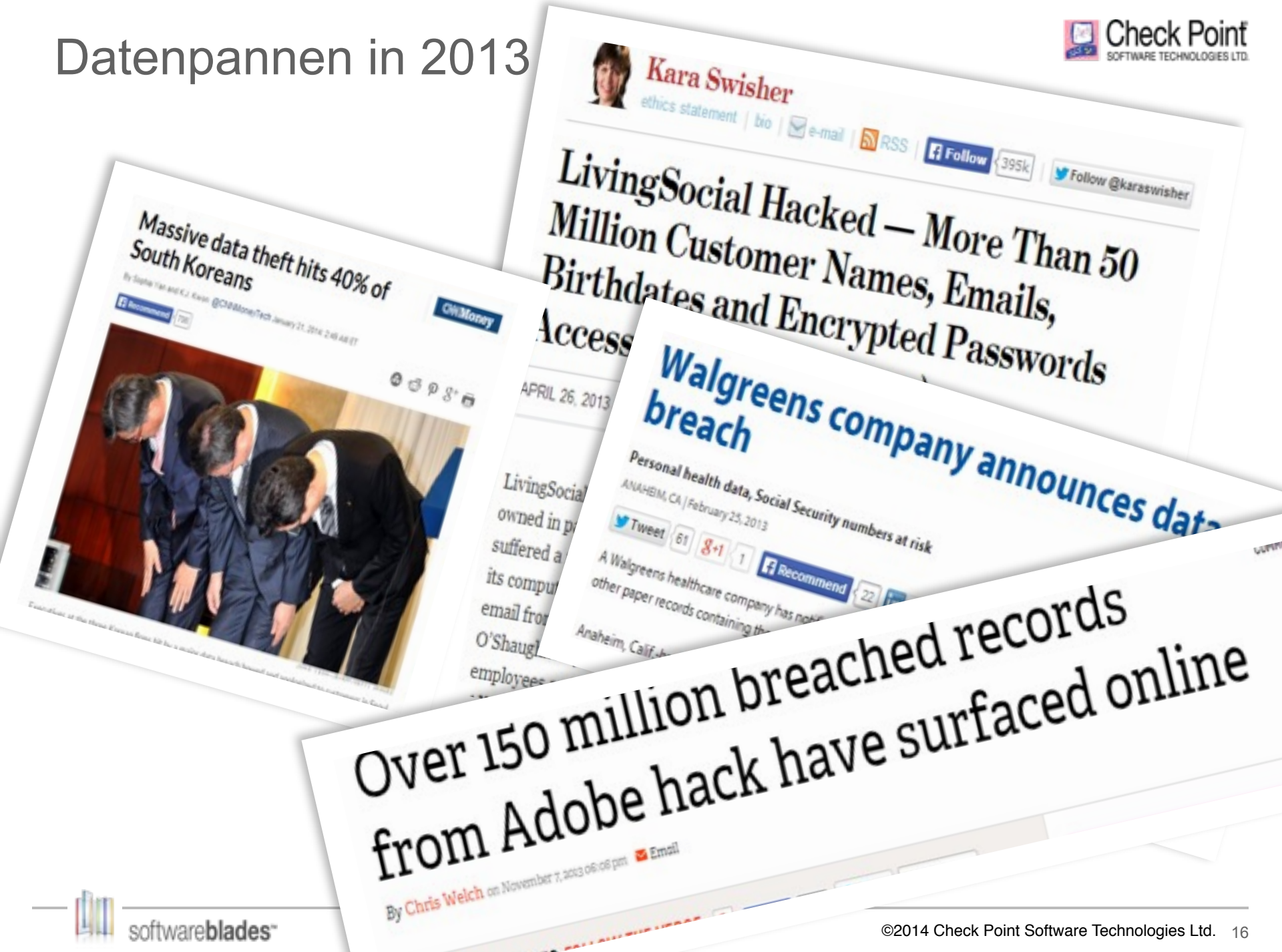
96% der Unternehmen haben mindestens eine risikoreiche Anwendung im Einsatz

Datenverlustvorfälle steigen stark an

- 88% der Unternehmen erlitten mindestens einen Datenverlust in 2013
- *Wirtschafts-spionage kostet amerikanische Unternehmen 250-500 Millionen $ pro Jahr*



Datenpannen in 2013



Stündliche Vorfälle im Unternehmensnetzwerk

- Sensible Daten verlassen das Unternehmen – **alle 49 Minuten**
- Unbekannte Malware wird geladen – **alle 27 Minuten**
- Bekannte Malware wird geladen – **alle 10 Minuten**
- Einsatz risikoreicher Anwendung – **alle 9 Minuten**
- Bot-Kommunikation mit seinem C&C Server – **alle 3 Minuten**
- Hostzugriff auf infizierte Web Seiten – **jede Minuten**

EINE STUNDE

Was müssen sie in 2014 tun ?

1

Der Einsatz unbekannter Schadsoftware explodierte in 2013
Integrierte Schadsoftware Sandbox ist ein Muss

Was müssen sie in 2014 tun ?

1

Der Einsatz unbekannter Schadsoftware explodierte in 2013
Integrierte Schadsoftware Sandbox ist ein Muss

2

Malwarevorfälle und Infizierung nehmen ständig zu
Anti-bot und Antivirus müssen globale Intelligenz besitzen

Was müssen sie in 2014 tun ?

1. Der Einsatz unbekannter Schadsoftware explodierte in 2013
   Integrierte Schadsoftware Sandbox ist ein Muss

2. Malwarevorfälle und Infizierung nehmen ständig zu
   Anti-bot und Antivirus müssen globale Intelligenz besitzen

3. Der Einsatz risikoreicher Applikationen steigt ständig
   Regelbasierte Applikationskontrolle muss umgesetzt werden

Was müssen sie in 2014 tun ?

1. Der Einsatz unbekannter Schadsoftware explodierte in 2013
   Integrierte Schadsoftware Sandbox ist ein Muss

2. Malwarevorfälle und Infizierung nehmen ständig zu
   Anti-bot und Antivirus müssen globale Intelligenz besitzen

3. Der Einsatz risikoreicher Applikationen steigt ständig
   Regelbasierte Applikationskontrolle muss umgesetzt werden

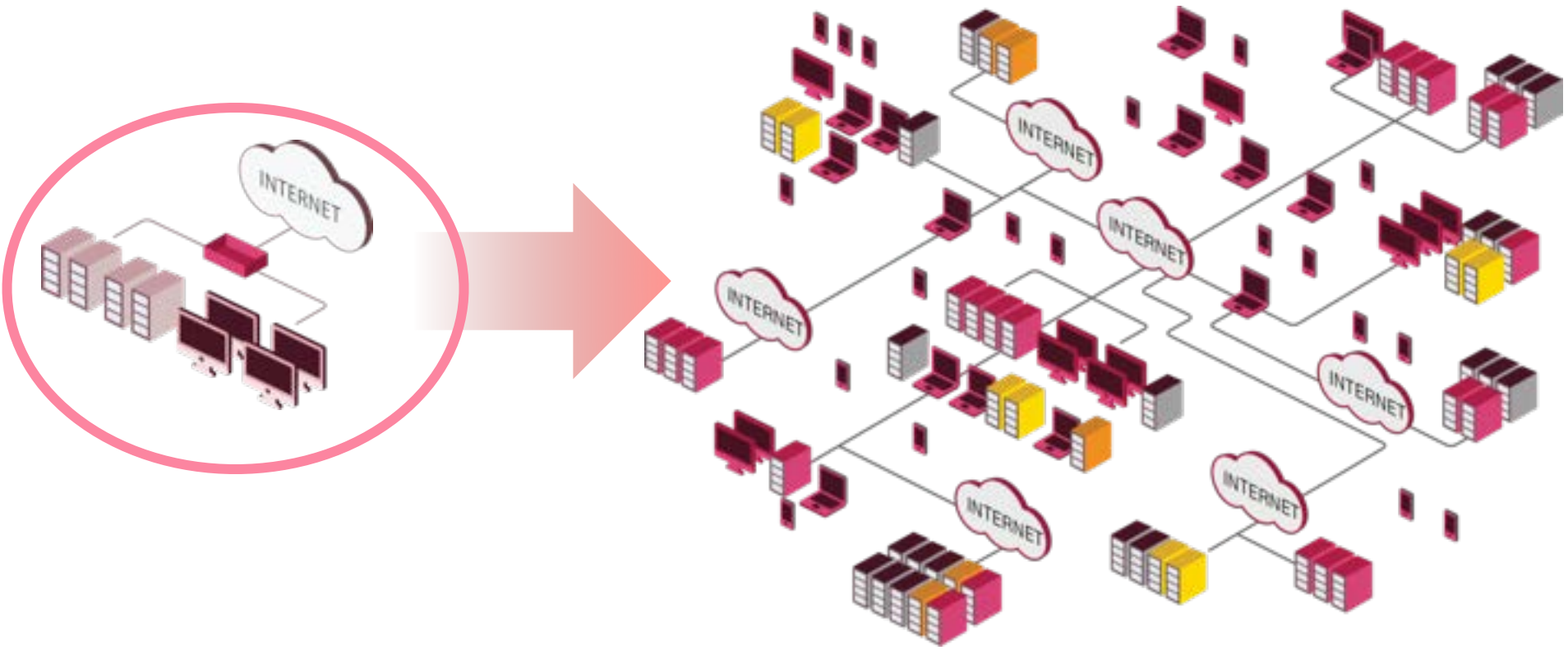
4. Datenverlust steigt: Unabhängig von Branche, Dateityp
   Ein DLP-Regelwerk muß zum Einsatz kommen

WIE SCHÜTZEN SIE IHR UNTERNEHMEN?

HEUTE

KOMPLEXE IT-UMGEBUNGEN

IT Umgebungen sind im Rahmen aufkommender Technologien gewachsen



SEGMENTIERUNG IST DER NEUE PERIMETER

In heutigen **NETZWERKEN**, gibt es keinen einzelnen Perimeter. Smartphones, Clouds und “moving User” **DATEN** kommunizieren über grenzenlose IT-Umgebungen

SDP

SOFTWARE DEFINED PROTECTION

Fragen?

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.