



CYBER SECURITY@DEUTSCHE TELEKOM






DR. MARKUS SCHMALL



ERLEBEN, WAS VERBINDET.

BEISPIELE WELTWEIT ERFOLGREICHER CYBER-ANGRIFFER

JEDES UNTERNEHMEN IST EIN MÖGLICHES OPFER

Diverse Rechner von internen Softwareentwicklern wurden infiziert	 	100 Millionen Kundendatensätze gestohlen, PSN für einen Monat außer Betrieb
Angreifer hatten über längeren Zeitraum Zugriff auf Rechner der Redaktion	 	Hoch entwickelte Trojaner Software auf PCs und Servern gefunden
250.000 Account-Daten mit Passwörtern gestohlen	 	IT-Attacke auf die Rüstungsindustrie
Diverse Rechner von internen Mitarbeitern wurden mit Schadsoftware infiziert	 	24 Millionen Kundendatensätze gestohlen
Erfolgreicher Angriff wurde bekannt gegeben, Details nicht veröffentlicht	 	Diebstahl interner und vertraulicher Kundendokumente (z.B. von FBI und NSA)
Zielgerichteter Angriff gegen einen Rüstungskonzern, Details nicht veröffentlicht	 	Diebstahl von 6,5 Mio. SHA 1 Passwort-Hashes
Angreifer hatten über Monate Zugriff auf Rechner in der Redaktion der NYT	 	Diebstahl von 2,5 Mio. MD5 Passwort-Hashes



TRANSPARENZ DURCH DAS SICHERHEITS-TACHOMETER WWW.SICHERHEITSTACHO.EU

ANALYSIERE DEINE ORGANISATION DURCH DIE AUGEN EINES ANGREIFERS.

T . . . ERLEBEN, WAS VERBINDET.

ÜBERSICHT EXPERTENMODUS INFO DOWNLOAD IMPRESSUM

Übersicht über die aktuellen Cyberangriffe (aufgezeichnet von 180 Sensoren)

Top 15 der Länder

Land	Anzahl der Angriffe
China	259.956
Canada	54.910

REALISIERBAR ALS KUNDENINDIVIDUELLES SENSOREN NETZWERK

WACHSTUM: INTERNATIONALER ROLLOUT

RUND 180 HONEYPOTS IN DEUTSCHE TELEKOM NETZWERK

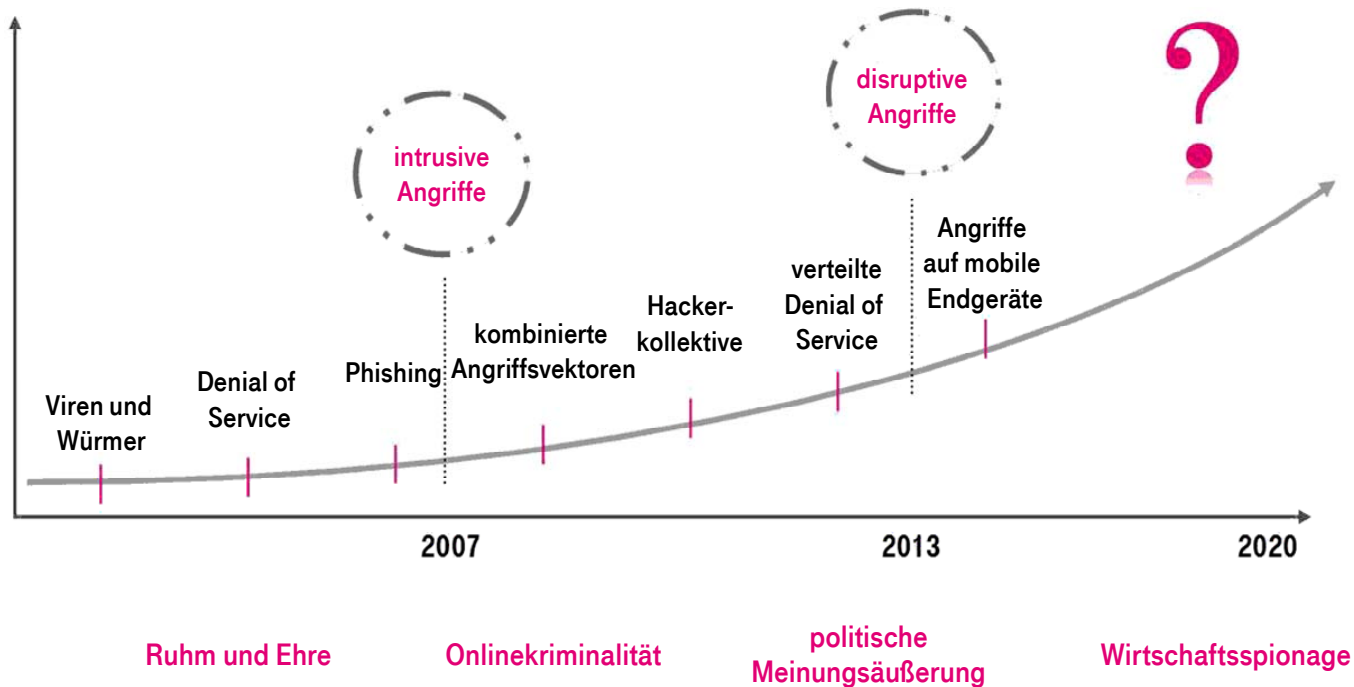
FESTSTELLUNG VON CA. 800.000 ANGRIFFEN PRO TAG

ECHTZEITÜBERBLICK VON ANGRIFFEN, TOP 15 LÄNDER UND VERTEILUNG VON ANGRIFFSZIELEN



ERLEBEN, WAS VERBINDET.

GLEICHZEITIG WERDEN ANGRIFFE IMMER PROFESSIONELLER UND DIE SCHÄDEN IMMER GRÖßER



Wachsende Angriffsberfläche

- Steigende IT Durchdringung erhöht das Risiko von Angriffen

Steigende Professionalität

- Hacker Community agiert hoch organisiert und zielgerichtet

Erhöhtes Ausmaß

- Schadensauswirkungen erstrecken sich über sämtliche Unternehmensbereiche

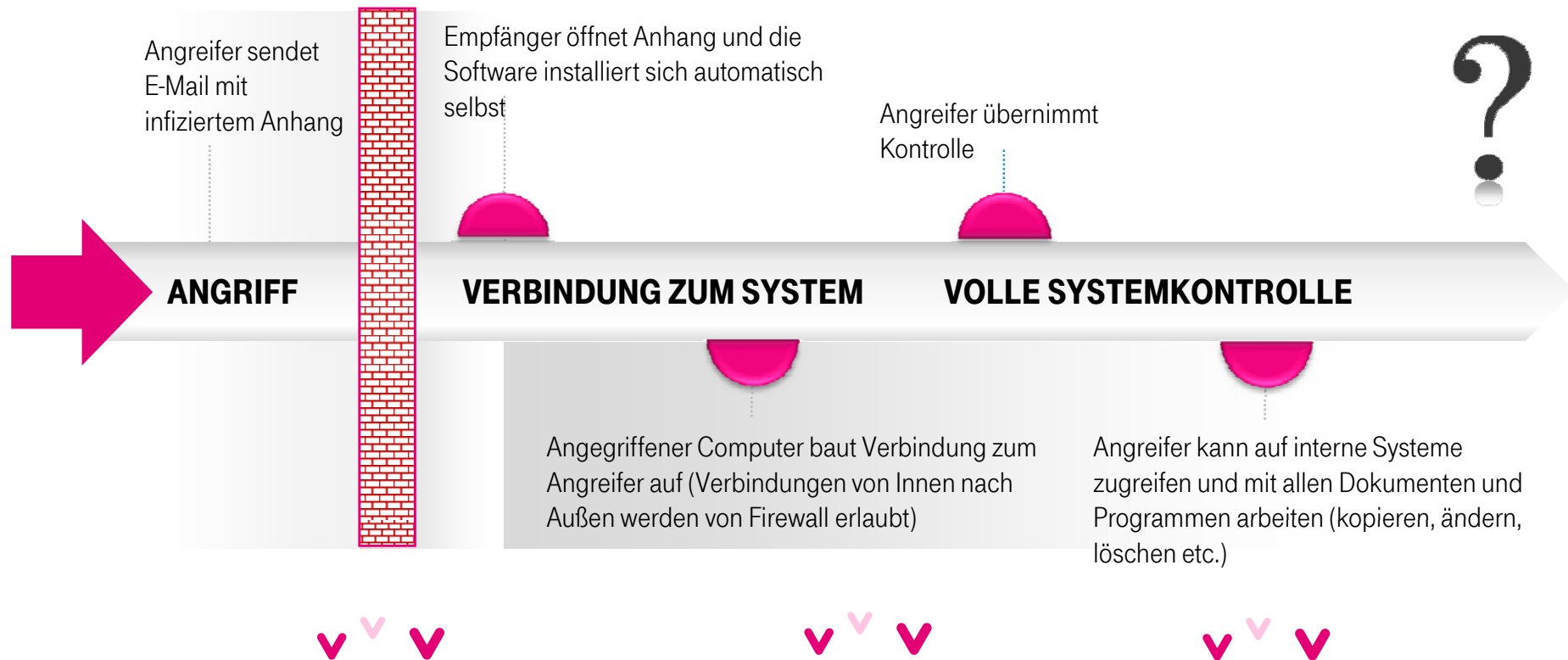


UNTERSCHIEDLICHE TYPEN VON ANGREIFERN ABER: GLEICHE METHODEN BEI DIVERGIERENDEN ZIELEN

	KLASSISCHE „HACKER“	ORG. KRIMINALITÄT	HACKTIVISTEN	NACHRICHTENDIENSTE
MOTIVATION 	<ul style="list-style-type: none"> Ruhm und Ehre Zeigen was man kann Spiel und Spaß 	<ul style="list-style-type: none"> Betrug Erpressung Geldwäsche 	<ul style="list-style-type: none"> Politische Meinungsäußerung 	<ul style="list-style-type: none"> Spionage Sabotage 
RESSOURCEN 	<ul style="list-style-type: none"> Zumeist Einzelpersonen 	<ul style="list-style-type: none"> Gut organisierte Gruppen Hohe Arbeitsteiligkeit Weltweite Verteilung Hohe Finanzmittel verfügbar 	<ul style="list-style-type: none"> Gut organisierte Gruppen Hohe Arbeitsteiligkeit Weltweite Verteilung 	<ul style="list-style-type: none"> Staatlich gelenkt Extrem hohe Finanzmittel verfügbar
BEISPIELE 	<ul style="list-style-type: none"> Verunstalten von Internetseiten Meldungen von Schwachstellen in Webseiten an die Presse ... 	<ul style="list-style-type: none"> Phishing-E-Mails DDoS auf Online-shops/Onlinewetten SPAM ... 	<ul style="list-style-type: none"> DDoS gegen Banken, die Wikileaks Konten gesperrt hatten Anonymous Angriffe auf Unternehmen ... 	<ul style="list-style-type: none"> Stuxnet (Iranisches Atomprogramm) Red October (Regierungen im Ostblock) ...

← Primärfokus der Sicherheitsarbeit →
← Sekundärfokus/Projektspezifisch →

ANGREIFER ARBEITEN HÖCHST ZIELGERICHTET UND SCHNELL



ES GIBT FÄLLE IN DENEN DER GANZE PROZESS - VOM ANGRIFF BIS ZUR ÜBERNAHME DER KONTROLLE - NUR 6 MINUTEN DAUERT !



NEUER TREND ANGRIFFSZIEL SMARTPHONE

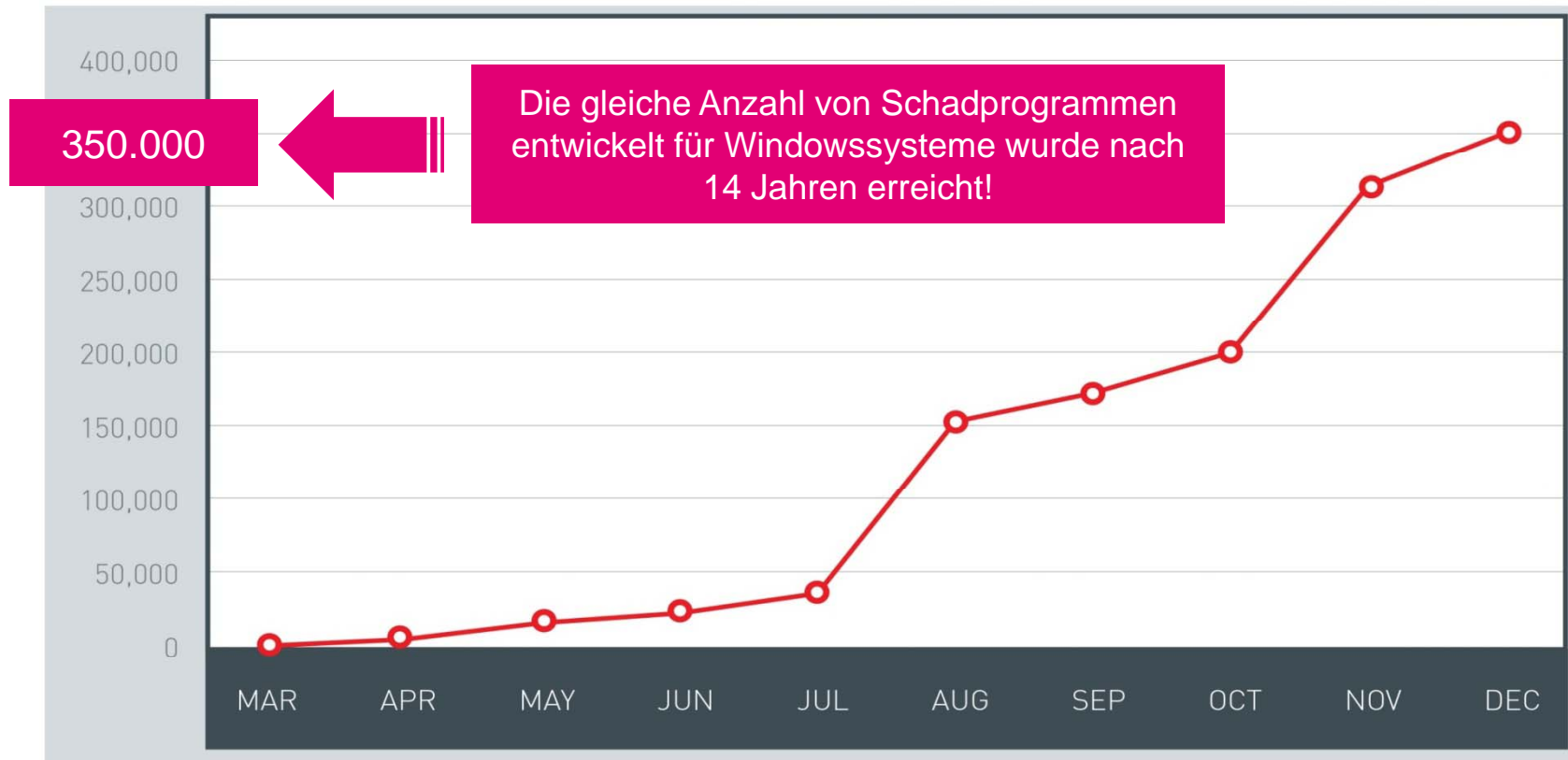
ALLE ENDGERÄTE-TYPEN BETROFFEN



BEOBACHTUNGEN DER HONEYPOTS

- Innerhalb eines Jahres wurde ein simuliertes Smartphone mehr als 300.000 mal attackiert.
- 330 dieser Angriffe waren erfolgreich, im Durchschnitt damit fast ein Angriff pro Tag.
- Weltweit werden derzeit fast eine Milliarde Smartphones genutzt.

ANGRIFFE AUF MOBILE GERÄTE MIT ANDROID ANZAHL SCHWACHPUNKTE WÄCHST EXPONENTIELL



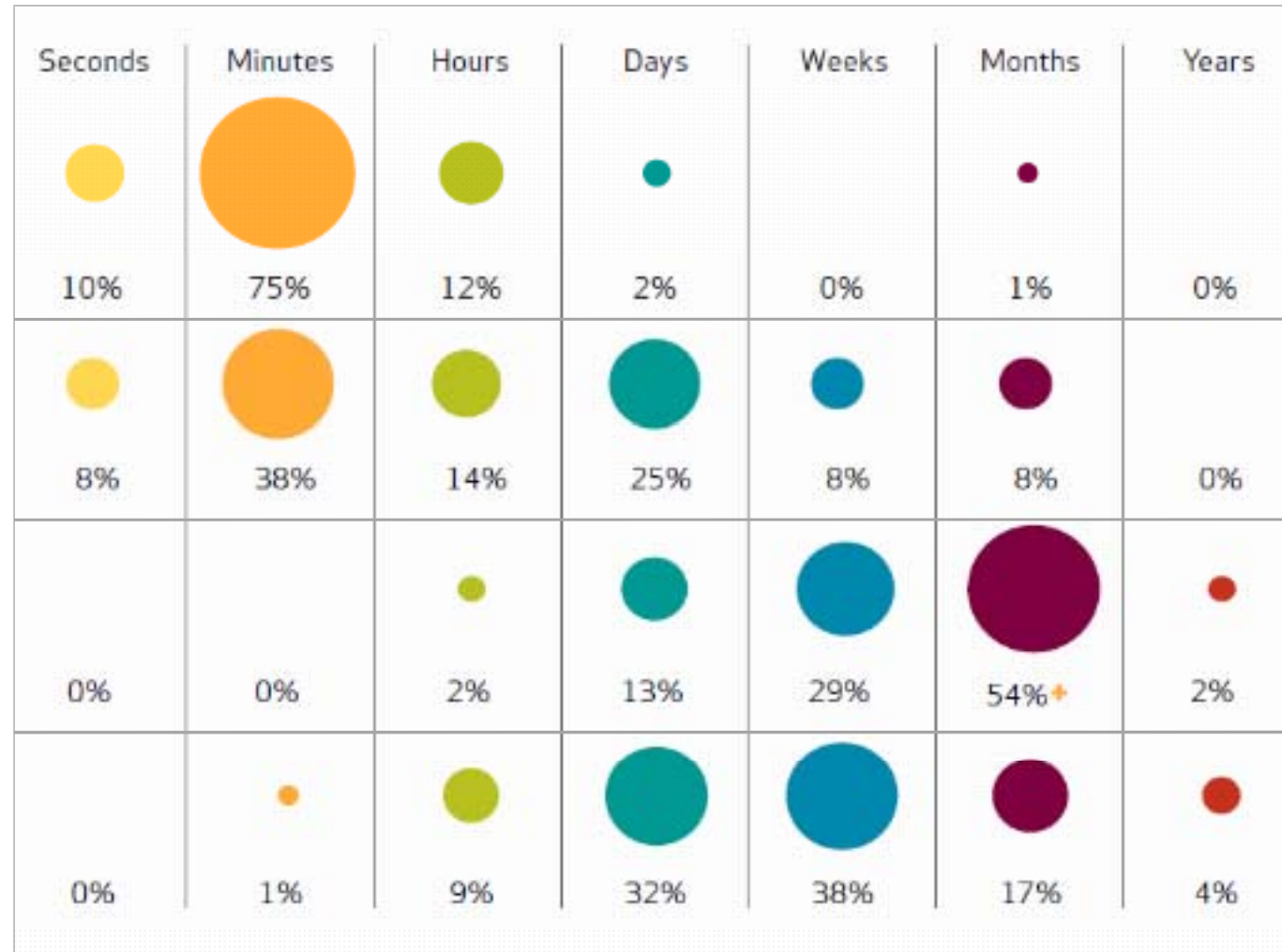
Quelle: Trend Micro Mobile Security Roundup 2012, Januar 2013



ERLEBEN, WAS VERBINDET.

VERIZON BREACH REPORT 2012 STELLT ZEITACHSE FÜR SYSTEMEINBRÜCHE DAR UND INDIZIERT DIE ANGRIFFSDAUER

**Dauer für
Angriffs-
Recherche**



**Dauer bis
Datenkompro-
mittierung
nach Einbruch**

**Dauer bis zur
Entdeckung
des Einbruchs**

**Benötigte Zeit
für Eindäm-
mung und
Bereinigung**



VERALTETE SOFTWARE IST DIE URSACHE FÜR DIE MEHRHEIT DER LETZTEN SICHERHEITSVORFÄLLE

SOFTWARE SCHWACHSTELLEN - MERKMALE



- Hohes Risiko aufgrund von Softwarefehlern
- Sicherheitsschwachstellen werden gnadenlos von Angreifern ausgenutzt
- Ein Durchschnitt von 400 neuen Schwachstellen werden pro Monat bekannt
- Rund 10% dieser Schwachstellen werden als "kritisch" eingestuft
- Unentdeckte Schwachstellen aufgrund gescheiterter Installation von Sicherheitsupdates



INCIDENTS - BEISPIELE



The Washington Post

The New York Times
Expect the World®



Microsoft

SONY

DRINGENDER BEDARF AN NEUER SICHERHEITSTECHNIK

<p>Großrechner</p> <p>1960</p>  <p>Benutzername Passwort</p> 	<p>Server</p> <p>1980</p>  <p>Firewall, Virus Schutz</p> 	<p>Mobile Computing</p> <p>1990</p>  <p>Intrusion Detection, WLAN-Encryption</p> 	<p>Smartphone Tablet PCs</p> <p>2005</p>  <p>SPAM Filter, Device Encryption</p> 	<p>Cloud Computing</p> <p>2010</p>  <p>Digitale Rechteverwaltung</p> 	<p>Seamless Computing</p> <p>2012</p>  <p>Honeypot Sensoren Mobile Security</p> 	<p>Internet of Things</p> <p>2014</p>  <p>Verhaltensbasierte Analyse</p> 
--	--	--	---	--	---	--

Zukünftige IT-Sicherheitstechnik setzt verstärkt auf verhaltensbasierte Analyse. Daraus ergeben sich neue Herausforderungen für Mitbestimmung und Datenschutz.

VIELEN DANK!



ERLEBEN, WAS VERBINDET.