Karl Otto Feger

„Honey-Sense
in Sachsen“

4. Kommunaler IT-Sicherheitskongress 2017

„Umsetzung der Leitlinie für Informationssicherheit des IT-Planungsrats in Kommunalverwaltungen“

STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Angriffserkennung im Netz

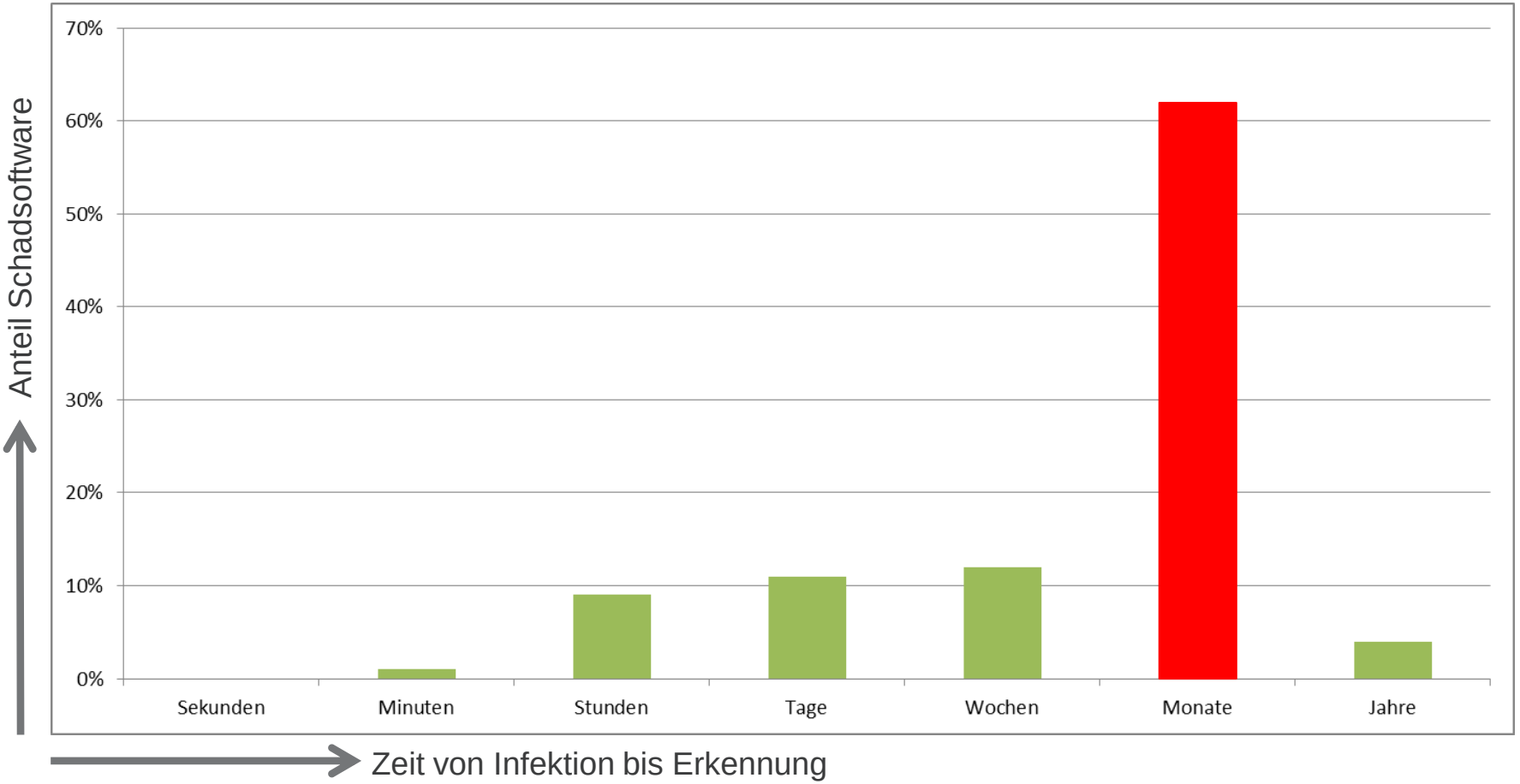
Projekt HoneySens

Meine Agenda für heute

- Wurden Sie heute schon gehackt?
- Anatomie eines Angriffs
- HoneySens
- Schlussbetrachtungen

Wurden Sie heute schon gehackt?

…oder haben Sie es (noch) gar nicht bemerkt?



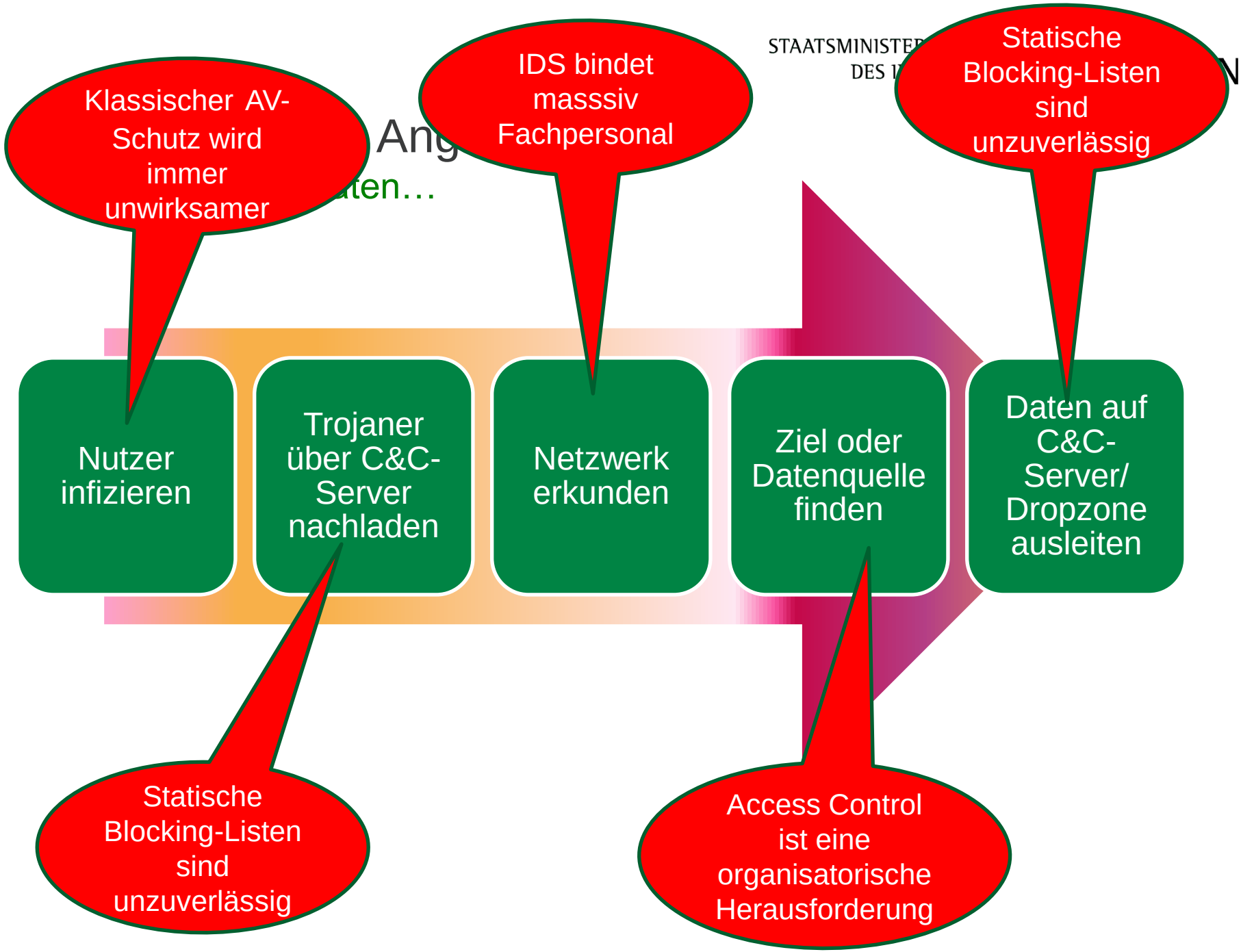
Quelle: Verizon Data Breach Report 2013

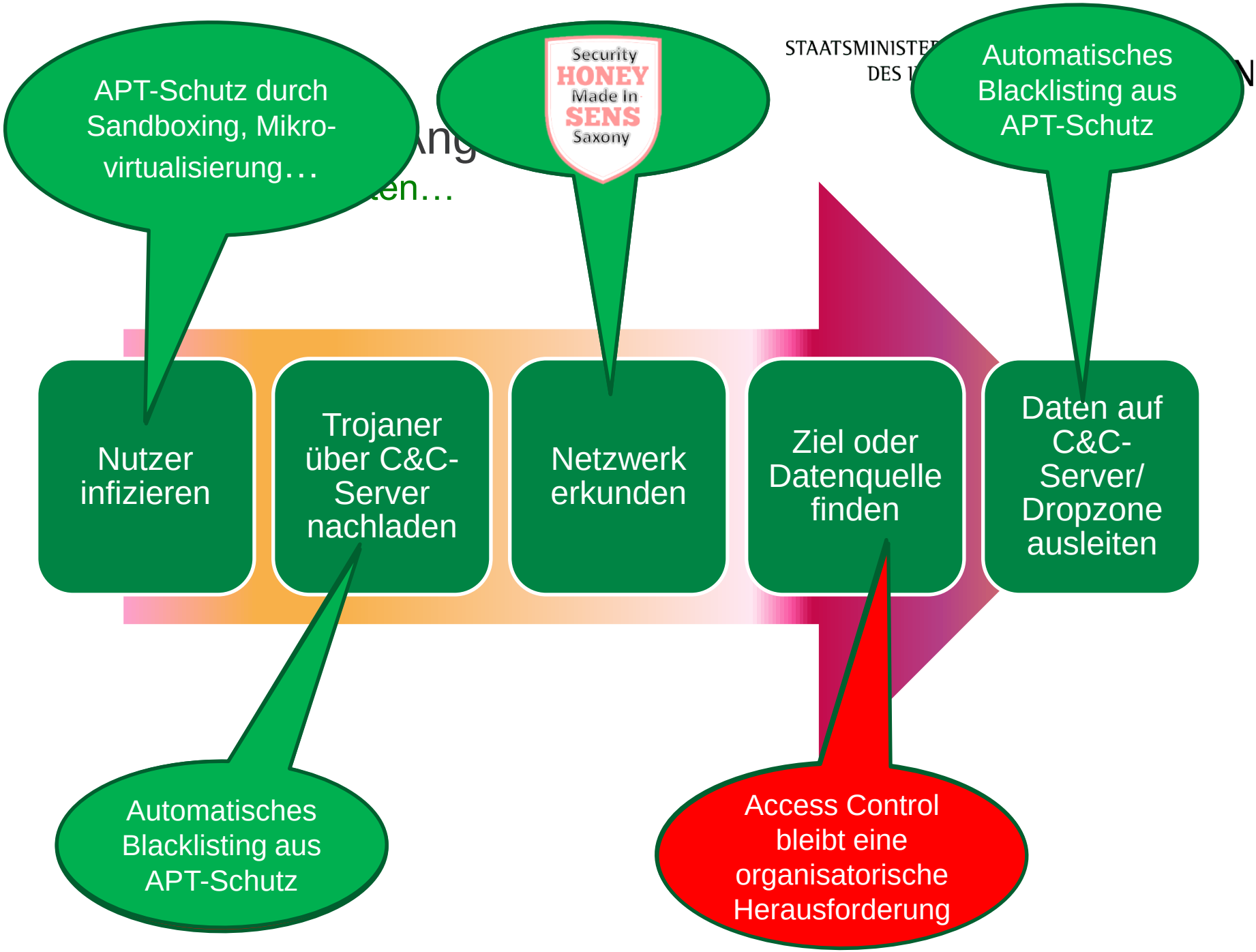
Wer greift an?

Quelle: IBM

Anatomie eines Angriffs

…gebt her Eure Daten…


Klassischer AV-Schutz wird immer unwirksamer
IDS bindet masssiv Fachpersonal
Statische Blocking-Listen sind unzuverlässig
Nutzer infizieren
Trojaner über C&C-Server nachladen
Netzwerk erkunden
Ziel oder Datenquelle finden
Daten auf C&C-Server/ Dropzone ausleiten
Statische Blocking-Listen sind unzuverlässig
Access Control ist eine organisatorische Herausforderung


APT-Schutz durch Sandboxing, Mikro-virtualisierung…
Security HONEY Made In SENS Saxony
Automatisches Blacklisting aus APT-Schutz
Nutzer infizieren
Trojaner über C&C-Server nachladen
Netzwerk erkunden
Ziel oder Datenquelle finden
Daten auf C&C-Server/ Dropzone ausleiten
Automatisches Blacklisting aus APT-Schutz
Access Control bleibt eine organisatorische Herausforderung

HoneySens
Ziele

- Angreifer und Angriffsmethoden durch Täuschung eines Angreifers im Netzwerk schnell erkennen. Sei dies ein Innentäter oder ein Eindringling im Netzwerk (Trojaner, RAT)
- Ablenkung des Angreifers von Produktivsystemen
- Zero-Day-Angriffe erkennen
- Benutzerfreundlich, einfache Wartbarkeit, hohe Vertraulichkeit etc.
- Vermeiden bisherige Nachteile wie
  - Hoher Installations- und Wartungsaufwand
  - Aufwändiges Monitoring
  - Hohe Kosten
- „HoneySens as a Service“-Modell soll möglich sein

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

HoneySens

Projektpartner

- Projektidee und Auftraggeber des Forschungsprojekts:
  Sächsisches Staatsministerium des Innern
  Referat 65 „Informationssicherheit in der Landesverwaltung, Cybersicherheit“

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

- Wissenschaftlicher Partner:
  Technische Universität Dresden
  Lehrstuhl für Datenschutz und Datensicherheit

TECHNISCHE UNIVERSITÄT DRESDEN

- Praxispartner:
  SAX.CERT
  im Staatsbetrieb Sächsische Informatik Dienste

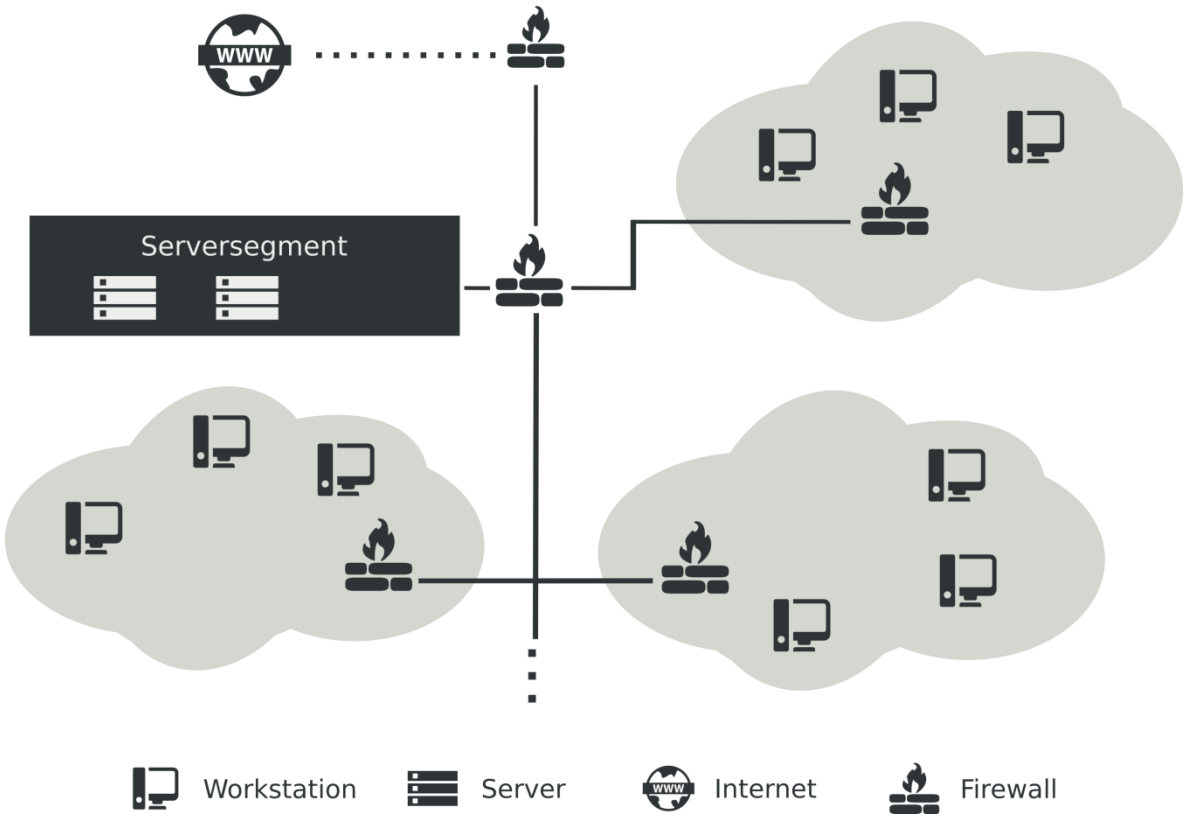
SAX.CERT Computer Emergency Response Team des Freistaates Sachsen

- Umsetzung:
  Dipl. Inf. Pascal Brückner im Rahmen seiner Diplomarbeit als Proof Of Concept und in der Fortsetzung zum produktionsreifen System als wissenschaftlicher Mitarbeiter der TU Dresden

Security HONEY Made In SENS Saxony

HoneySens

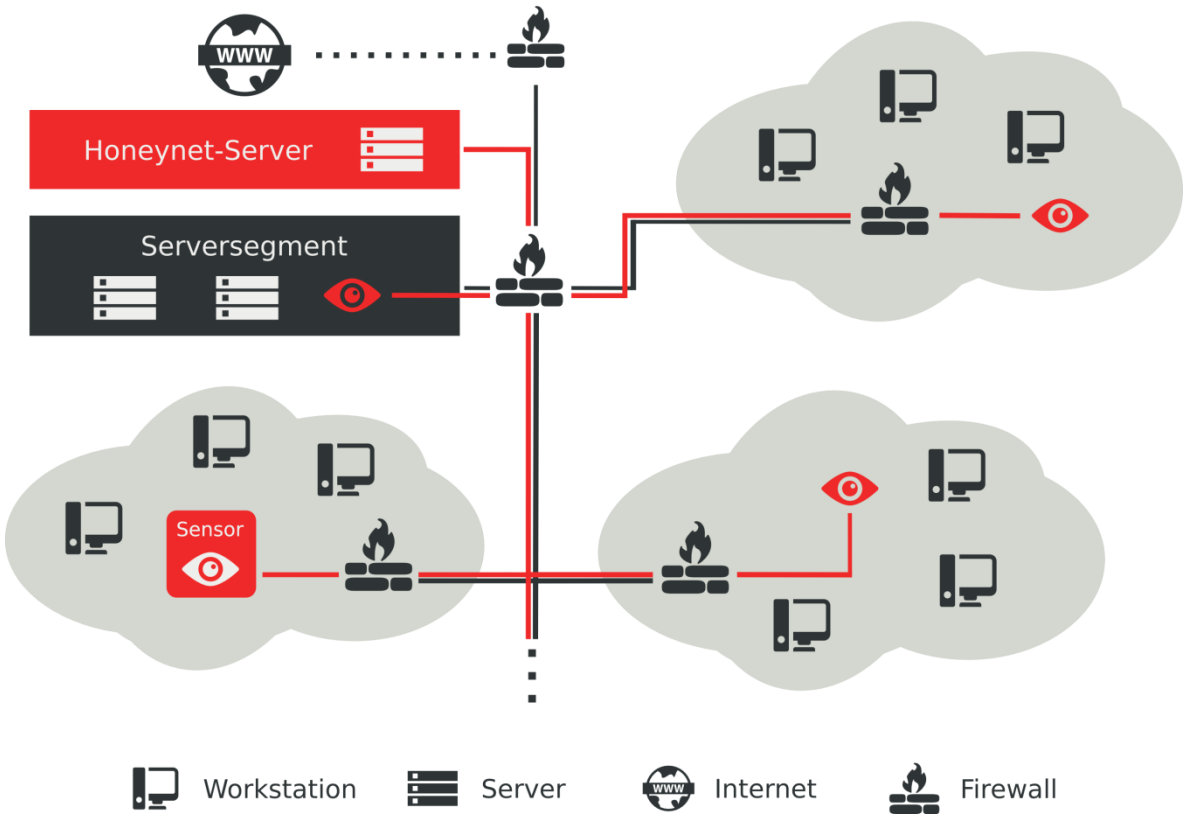
Architektur



Security HONEY Made In SENS Saxony

HoneySens

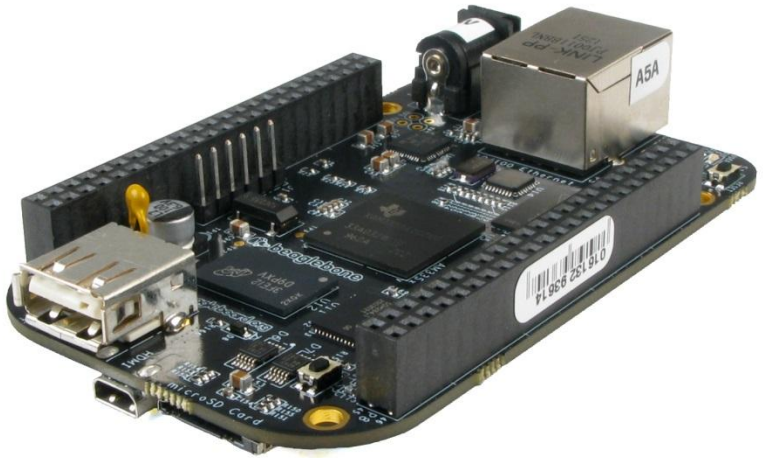
Architektur



HoneySens

Die Sensoren

- **Hardwareplattform**: Einplatinen-Computer BeagleBone Black (ARM)
- Preiswert, geringer Stromverbrauch, Formfaktor, integrierter persistenter Festspeicher, optionales PoE
- **Softwareplattform**: Debian GNU/Linux
- Hochwertig gesicherte Client-/Server-Kommunikation
- Remote-Installation und Remote-Update
- Low-Interaction-Honeypot-Dienste: kippo (SSH), dionaea (SMB/CIFS)
- Passive Scan Mode zur Aufzeichnung aller übrigen Verbindungsversuche
- Portscan-Erkennungsroutine

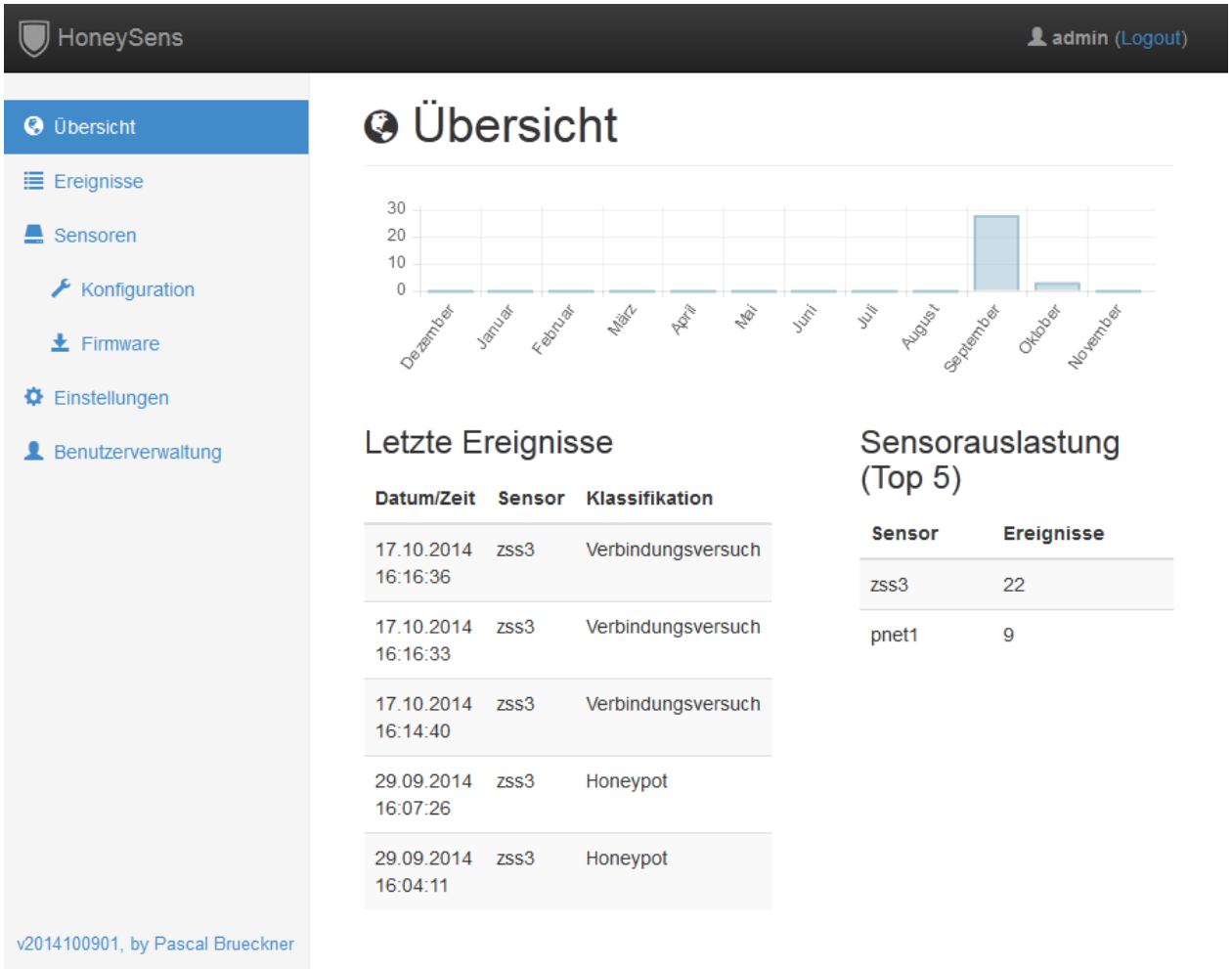


HoneySens
Der Server

- Linux-System mit geringer bis mittlerer Leistung
  - Betrieb als virtuelles System möglich
- Einsatz von Docker für den vereinfachten Roll-Out und aufwandsarme Updates
- Mandaten-fähiges System
  - z.B. Land – Ressorts – Kommunen auf gleichem Server bei beibehaltener Eigenverantwortung
- E-Mail-Alarmierung der jeweils zuständigen Administratoren

HoneySens

Web-Frontend (1)



HoneySens

Web-Frontend (2)

Ereignisse

Update in 6s

Suchen:

ID	Zeitpunkt	Sensor	Klassifikation	Quelle	Details	Status	Aktionen
259	17.10.2014 16:16:36	zss3	Verbindungsversuch	192.168.1.195	UDP Port 1714	Neu	
254	29.09.2014 16:04:11	zss3	Honeypot	192.168.1.10	SMB/CIFS (dionaea)	Neu	
252	29.09.2014 15:33:17	zss3	Verbindungsversuch	192.168.1.10	TCP Port 123	Neu	
250	26.09.2014 18:06:31	zss3	Verbindungsversuch	192.168.1.10	TCP Port 999	Erledigt	
247	11.09.2014 18:28:47	zss3	Verbindungsversuch	192.168.1.10	TCP Port 123	Neu	
245	11.09.2014 18:24:00	zss3	Honeypot	192.168.1.10	SSH Port 22 (kippo)	Neu	
244	11.09.2014 17:32:23	zss3	Honeypot	192.168.1.10	SSH Port 22 (kippo)	Neu	
243	11.09.2014 17:11:24	zss3	Portscan	192.168.1.10	586 Pakete	Neu	
242	11.09.2014 17:11:12	zss3	Portscan	192.168.1.10	10 Pakete	Neu	
241	11.09.2014 16:03:12	zss3	Honeypot	192.168.1.10	SSH Port 22 (kippo)	Neu	
240	11.09.2014 16:01:52	zss3	Honeypot	192.168.1.10	SSH Port 22 (kippo)	Neu	
220	11.09.2014 12:07:58	zss3	Verbindungsversuch	192.168.1.10	TCP Port 123	Neu	

1 bis 12 von 12 Einträgen

Zurück 1 Nächste

Security HONEY Made In SENS Saxony

Evaluation

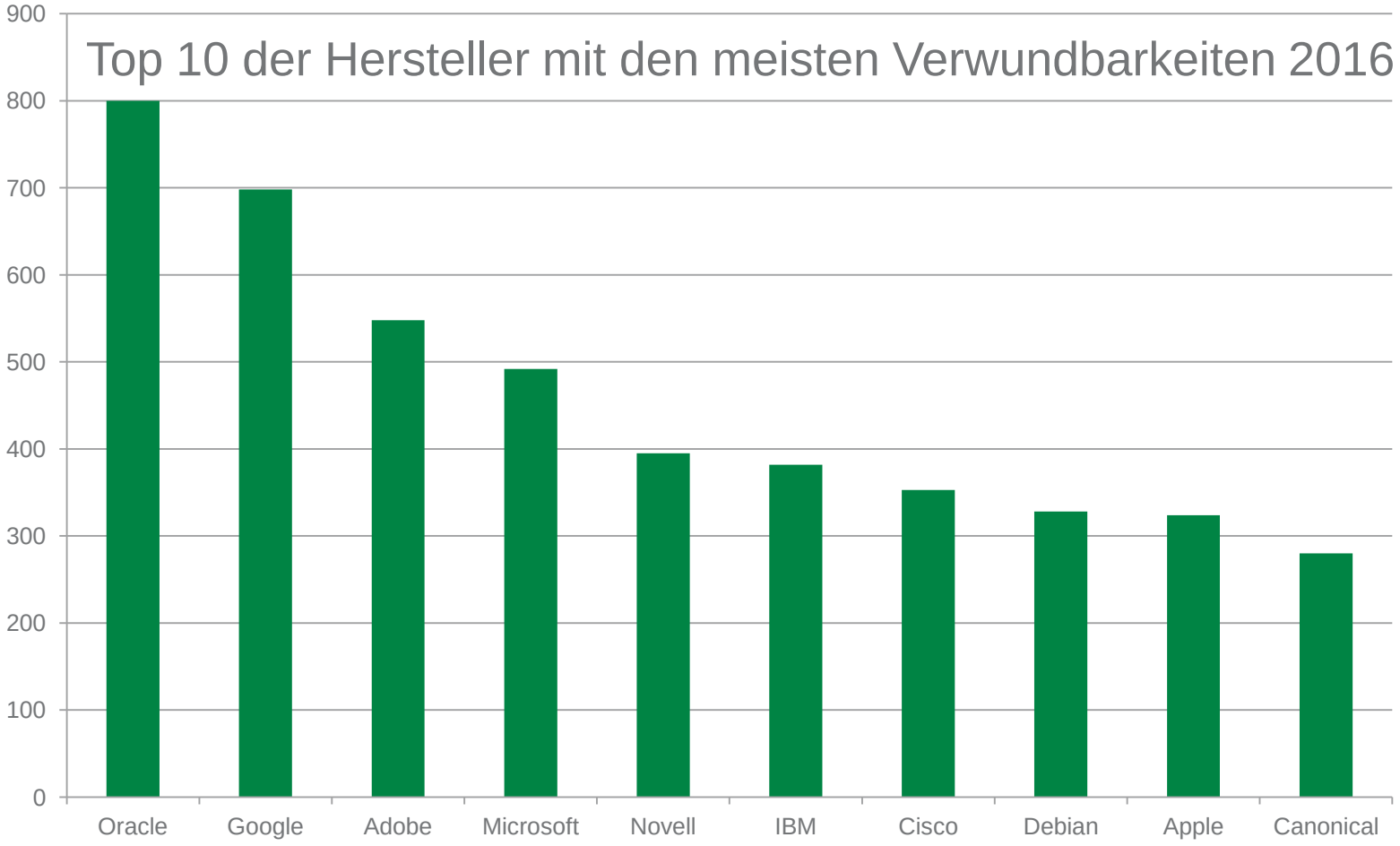
- **Erste Testumgebung**
  - SMI: ein Sensor im Produktivnetz
  - SID: vier Sensoren im Produktivnetz
  - Fakultät Informatik: ein Sensor für drei Wochen
- **Auswertung:**
  - SMI: ein Vorfall eines falsch konfigurierten Servers
  - Fakultät Informatik: 523 Ereignisse, davon 503 harmlose DHCP-Pakete
- **Funktionalität und Transparenz sind gegeben**
- Weitere Planung
  - Einsatz in allen Unternetzen des Sächsischen Verwaltungsnetzes sowie bei den Kommunen (auf freiwilliger Basis)

Security HONEY Made In SENS Saxony

Schlussbetrachtung

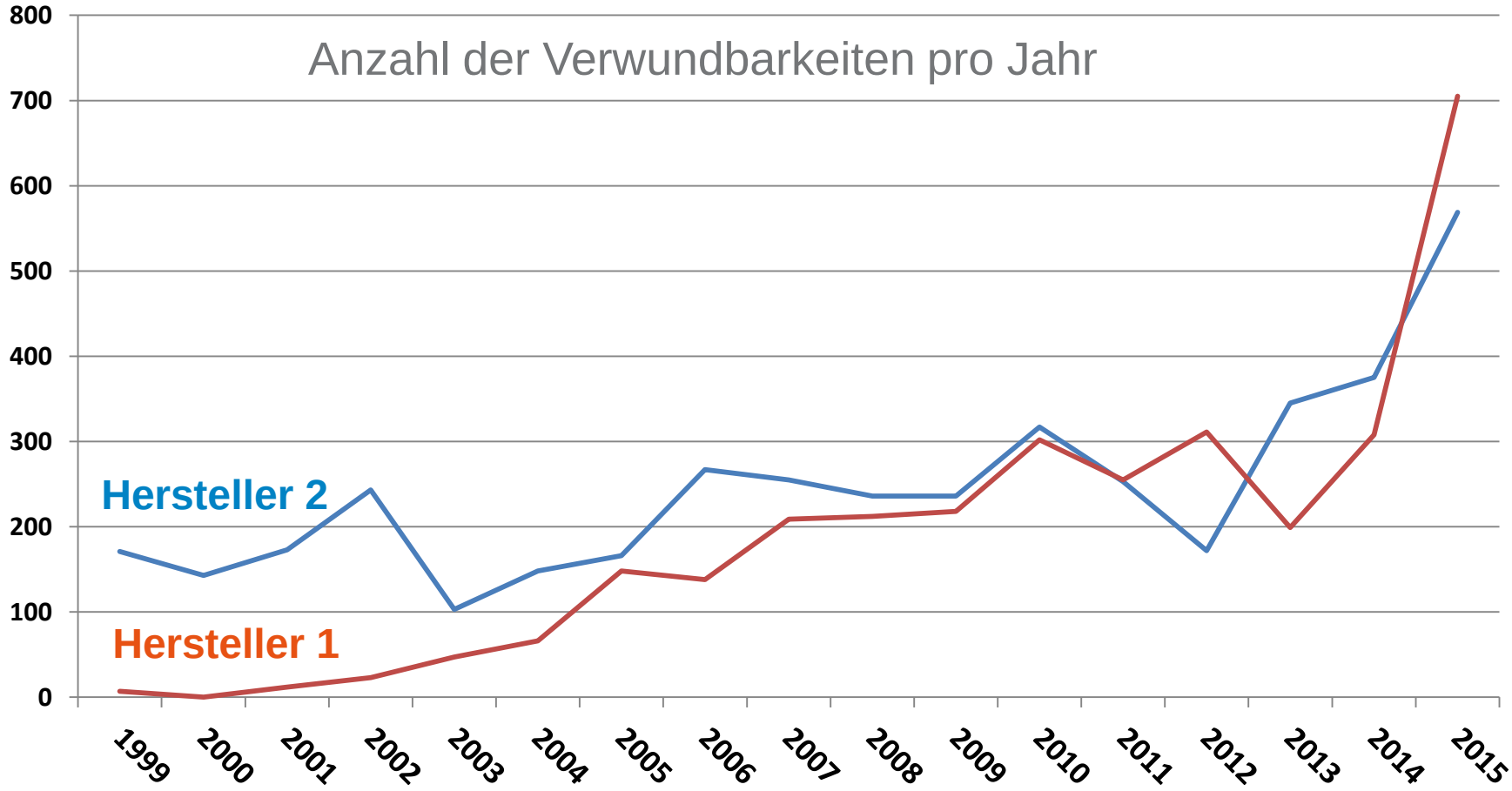
- HoneySens ist als kostengünstiges, leicht managebares Sensornetzwerk zur Erkennung von Netzwerkschnüfflern realisiert
- Das System wird den gestellten Anforderungen gerecht
- Fortsetzung der Zusammenarbeit mit der Technischen Universität Dresden zur weiteren Verbesserung und Härtung des Systems HoneySens, z.B.
  - Sensor als virtuelle x86-Maschine (interessant für Rechenzentren)
  - Integration in SIEM
- Übergang vom Forschungsprojekt zum käuflichen Produkt ist erfolgt
  - Entwicklung von Geschäftsmodellen, z.B. HoneySens as a Service
- Open Source-Version via GitHub wird auch verfügbar sein

So ganz nebenbei…
Warum konnten Sie eigentlich gehackt werden?



Quelle: Top 10 aus https://www.cvedetails.com/top-50-vendors.php?year=2016

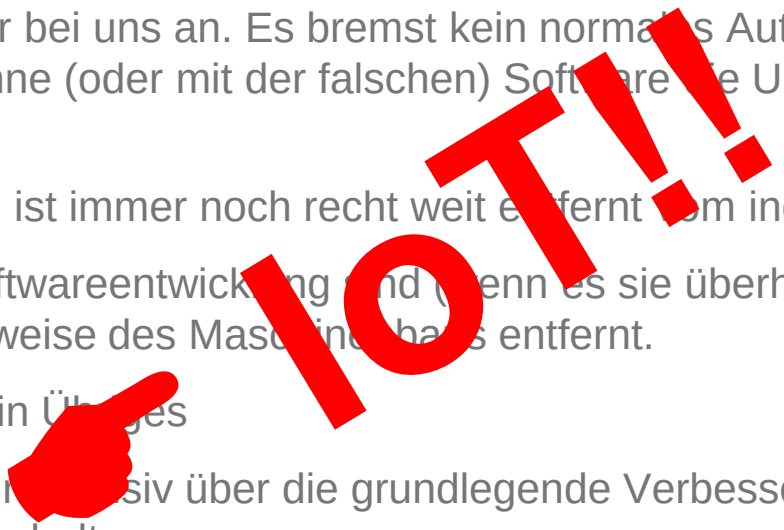
Warum konnten Sie eigentlich gehackt werden?



Quelle: https://www.cvedetails.com/

Schlussbetrachtung zum Zweiten

- Software ist mittlerweile zu einer der wichtigsten Plattformen unserer modernen Zivilisation geworden. Denn mittlerweile kommt ohne Software kein Wasser, kein Gas und kein Strom mehr bei uns an. Es bremst kein normales Auto mehr ohne Software, Motoren belasten ohne (oder mit der falschen) Software die Umwelt weit stärker als nötig.
- Software-Produktion ist immer noch recht weit entfernt vom ingenieurmäßgen Arbeiten.
- Standards in der Softwareentwicklung sind (wenn es sie überhaupt gibt) weit von den Standards beispielsweise des Maschinenbaus entfernt.
- Time to Market tut ein Übriges
- Wir müssen uns sehr intensiv über die grundlegende Verbesserung von Softwarequalität unterhalten.
- Wir werden uns ernsthaft über Fragen der Produkthaftung für Software-Hersteller unterhalten müssen.
- Es ist in diesem Zusammenhang unerheblich, ob wir über Closed Source oder Open Source sprechen.




Vehicle to Vehicle Communication
Internet/ PSTN
Engine Control Unit
Airbag Control Unit
Telematics
Transmission Control Unit
Body Controller Locks/Lights/Etc
Radio
TPMS
Antilock Braking System
OBD-II
Anti-Theft
HVAC
Keyless Entry
hue
PHILIPS
IT-Sicherheit wird nicht einfacher...
Facebook
Netflix
Hulu Plus
Samsung Apps
Your Video
Family Story
Fitness
Kids
Web Browser
USA TODAY
Pandora
AllShare Play
ESPN ScoreCenter
AccuWeather
Login
WallPaper
Tools
Return
nest
72

Karl-Otto Feger
Referatsleiter 65
CISO Sachsen
Sächsisches Staatsministerium des Innern
karl-otto.feger@smi.sachsen