Information und Technik
Nordrhein-Westfalen

Bedrohungslage und Gegenmaßnahmen Bestandsaufnahme aus CERT-Sicht

Fachforum VII: IT-Bedrohungen in der Verwaltung 4.0 begegnen: Prävention, Detektion, Reaktion

Dr. Jörg Flüs, Geschäftsbereichsleiter IT-Planung und Steuerung

Bedrohungen 2016 (ein ganz normaler Monat)

All Alarms by Priority

Time Window: *2016-10-07 14:22:23 - 2016-11-07 13:22:23*
Constraints: *Source / Destination IP* = [redacted]

Priority	Count
high	76,007
medium	176,122
low	759

SB1 by Priority

Time Window: *2016-10-07 14:22:23 - 2016-11-07 13:22:23*
Constraints: *Source / Destination IP* = [redacted]

Priority	Count
high	54,086
medium	161,023
low	619

SB2 by Priority

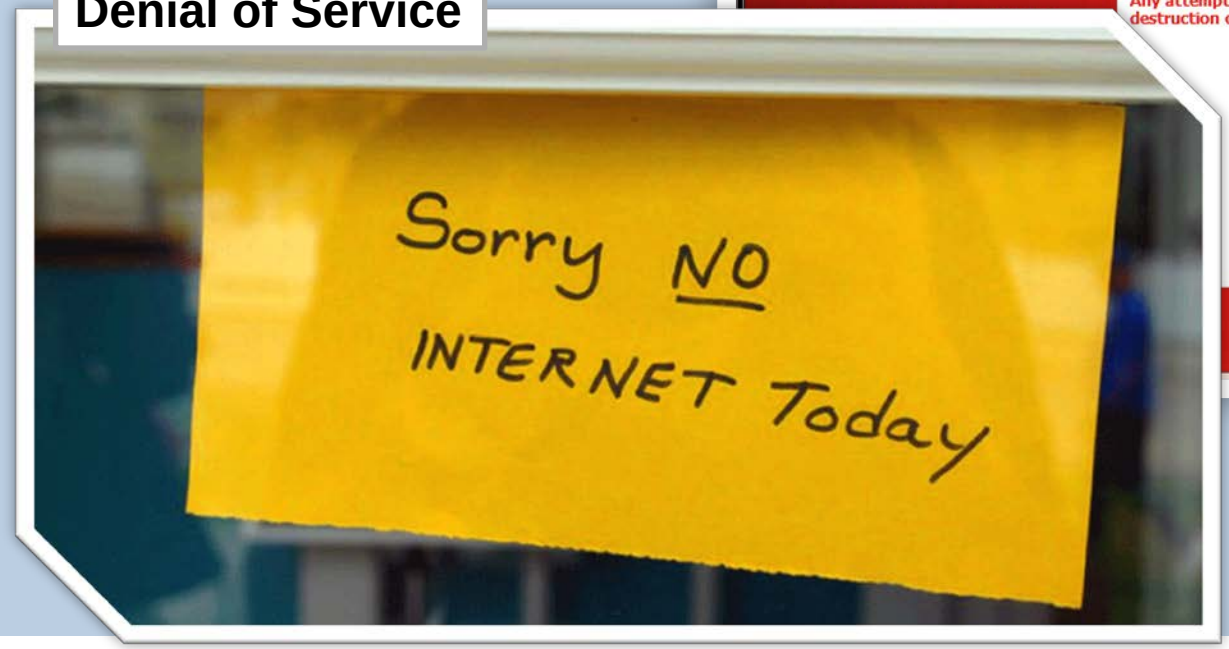
Time Window: *2016-10-07 14:22:23 - 2016-11-07 13:22:23*
Constraints: *Source / Destination IP* = [redacted]

Priority	Count
high	21,921
medium	15,099
low	140

Bedrohungen 2016

Ransomware

Denial of Service



Das ist nicht alles!

- Datendiebstähle/-manipulationen
- Phishing
- Vandalismus
- …
- Advanced Persistent Threats

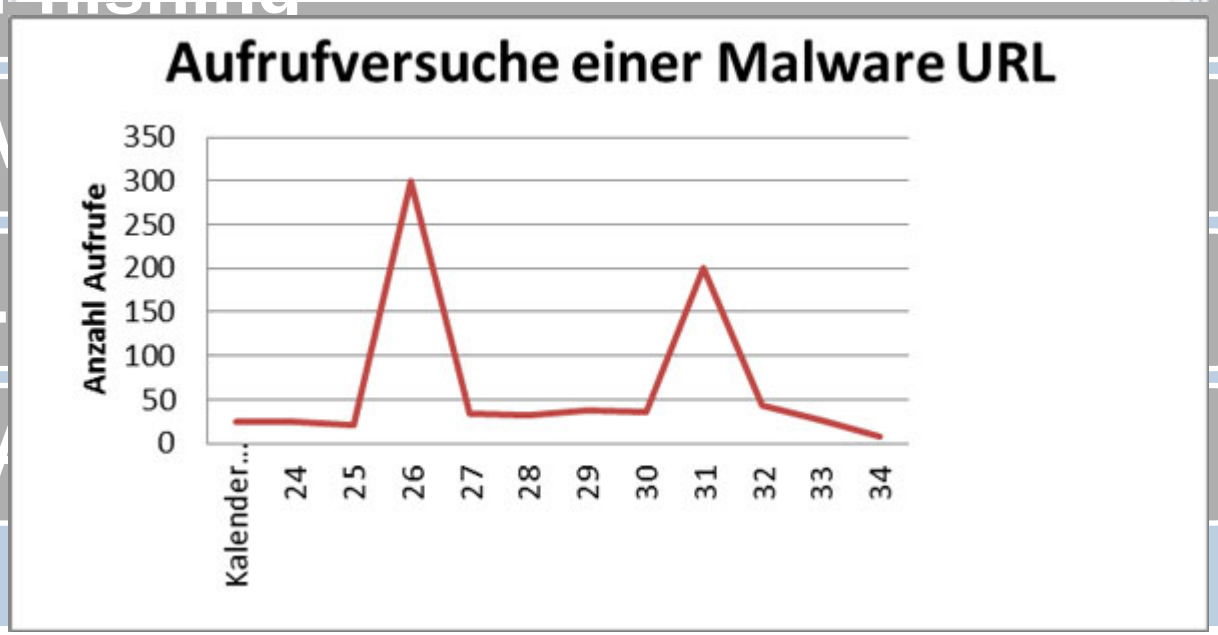
Das ist nich

Betreff: WG: RE:

Von: ella guttman [mailto:ellaguttman@[redacted]
Gesendet: Montag, 8. August 2016 07:45
An: [redacted]
Betreff: RE:

http://novel.oceansidegrill.com/

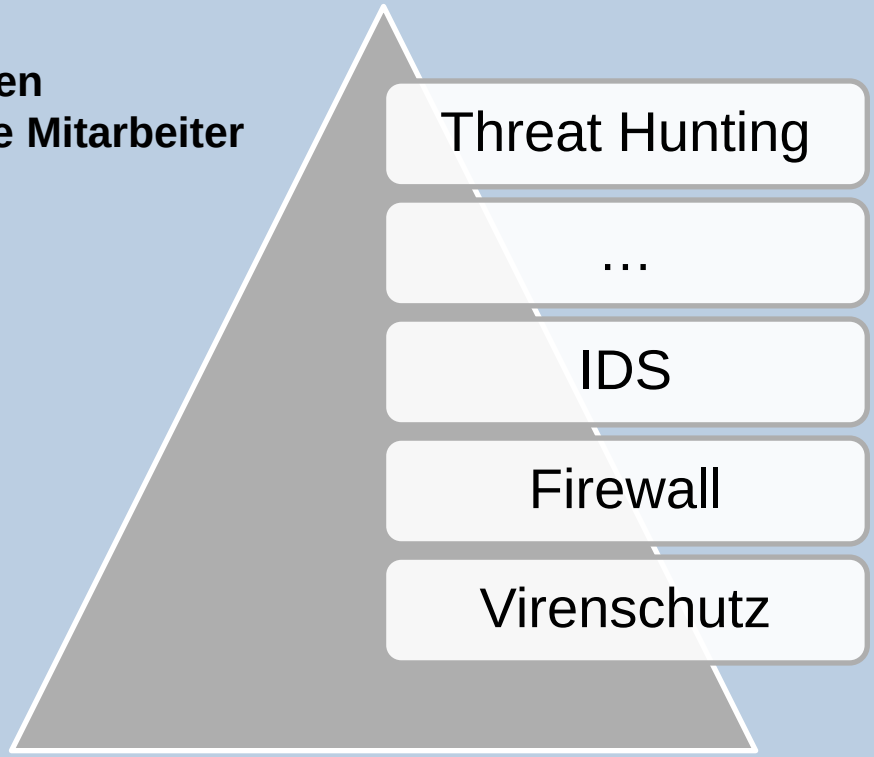
Ella Guttman



Gegenmaßnahmen

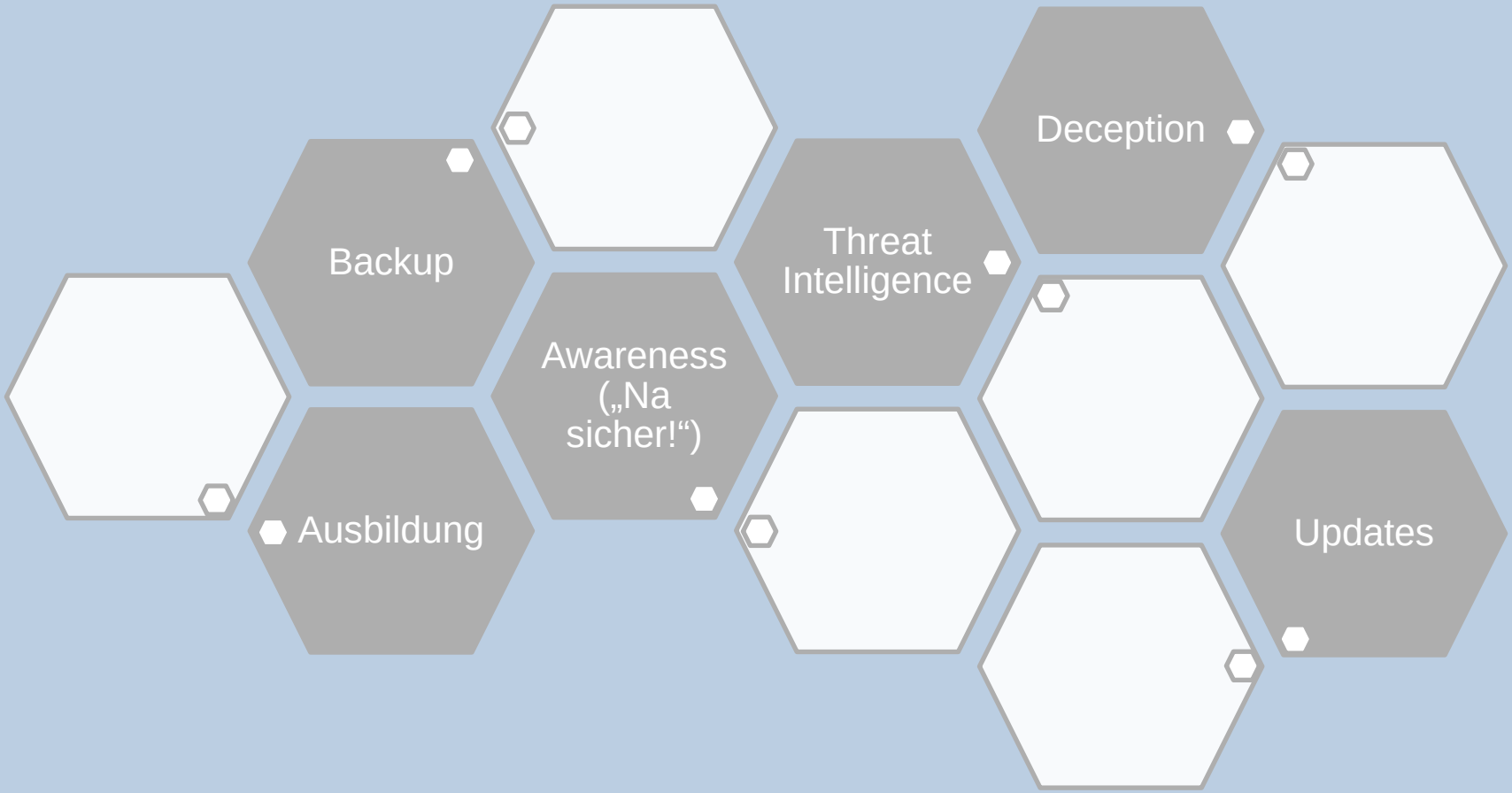
Detektion

- **nicht nur Appliances**
- **Gesamtkomplexität gering halten**
- **gut ausgebildete und motivierte Mitarbeiter**



Reaktion

Prävention


Backup
Threat Intelligence
Deception
Awareness („Na sicher!“)
Ausbildung
Updates

Fazit

Wir machen es den Angreifern noch zu leicht.

Das wollen wir ändern.