



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



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

Denial of Service

Sorry NO
INTERNET Today



Das ist nicht alles!

Datendiebstähle/-manipulationen

Phishing

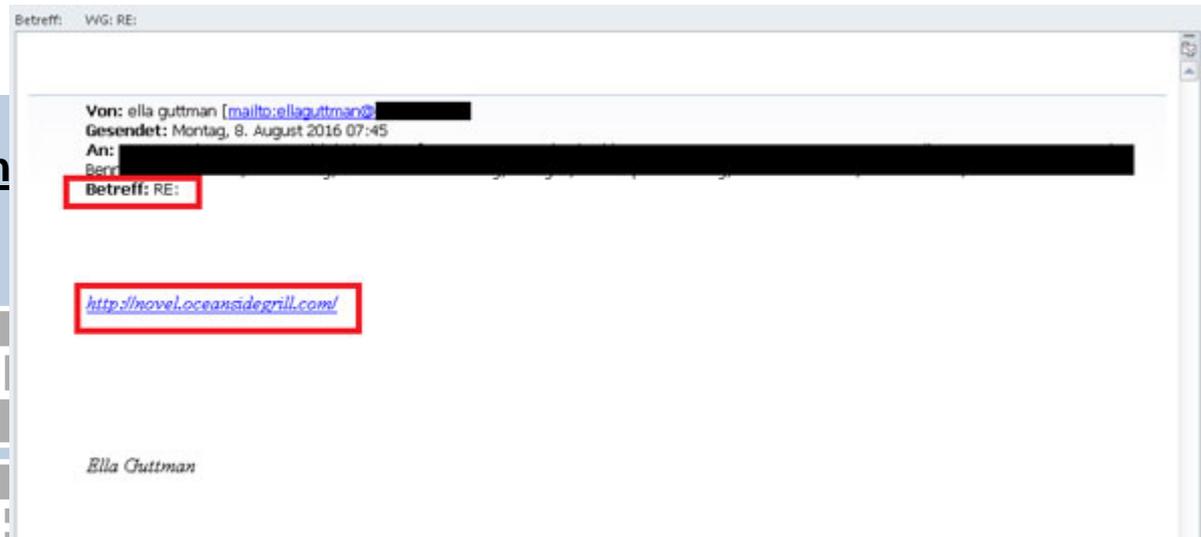
Vandalismus

...

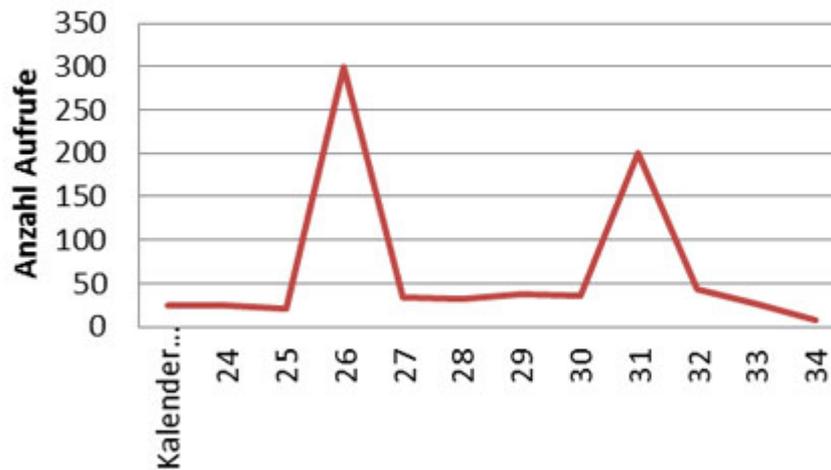
Advanced Persistent Threats



Das ist nicht

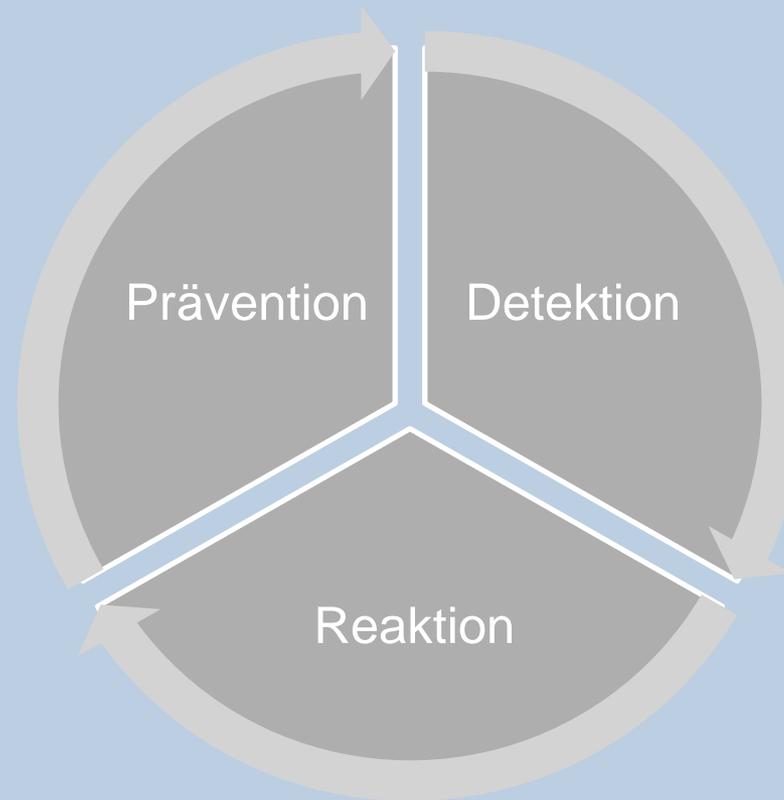


Aufrufversuche einer Malware URL





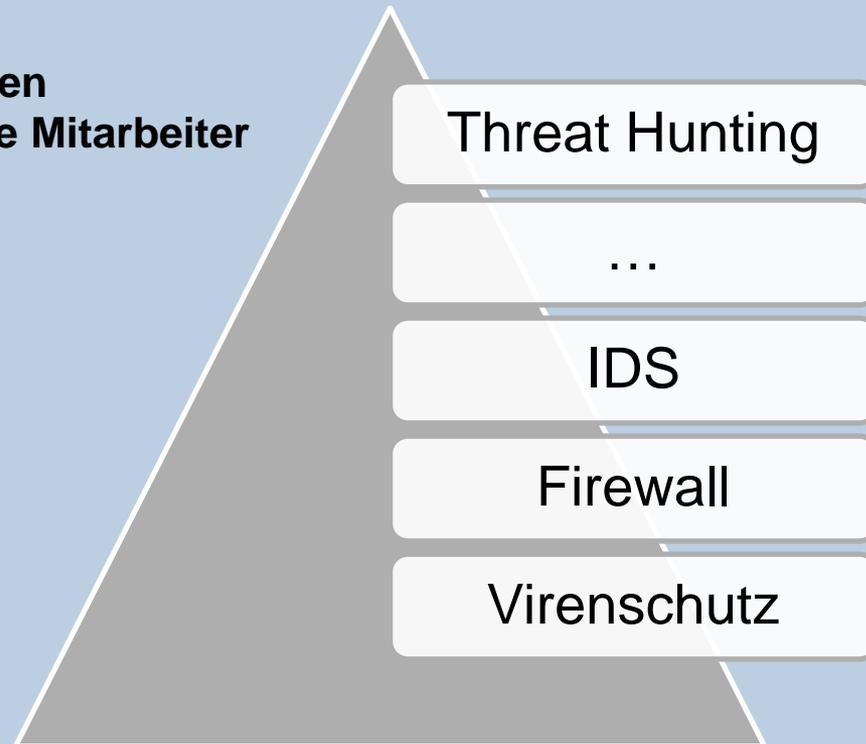
Gegenmaßnahmen





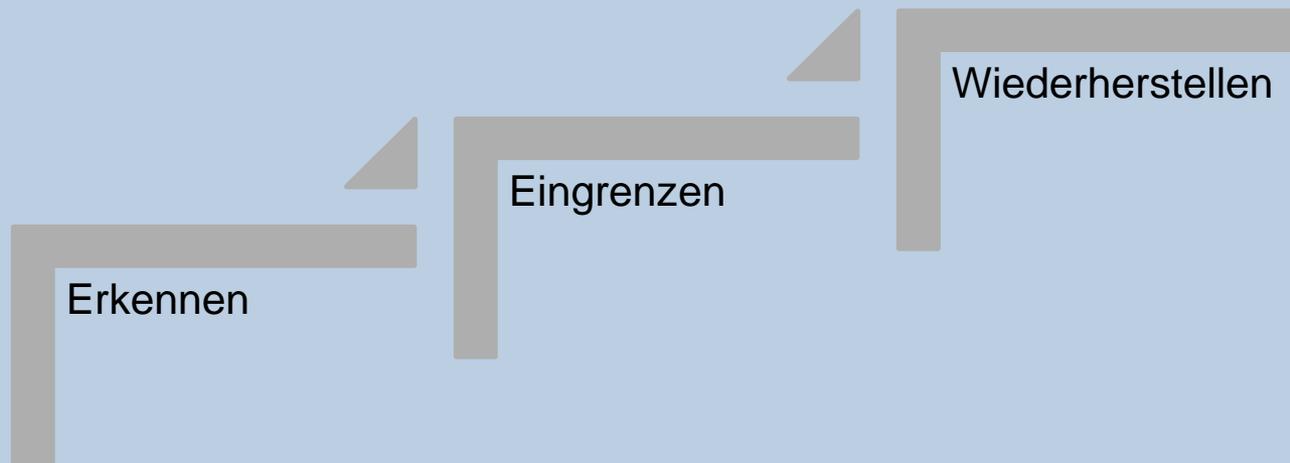
Detektion

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



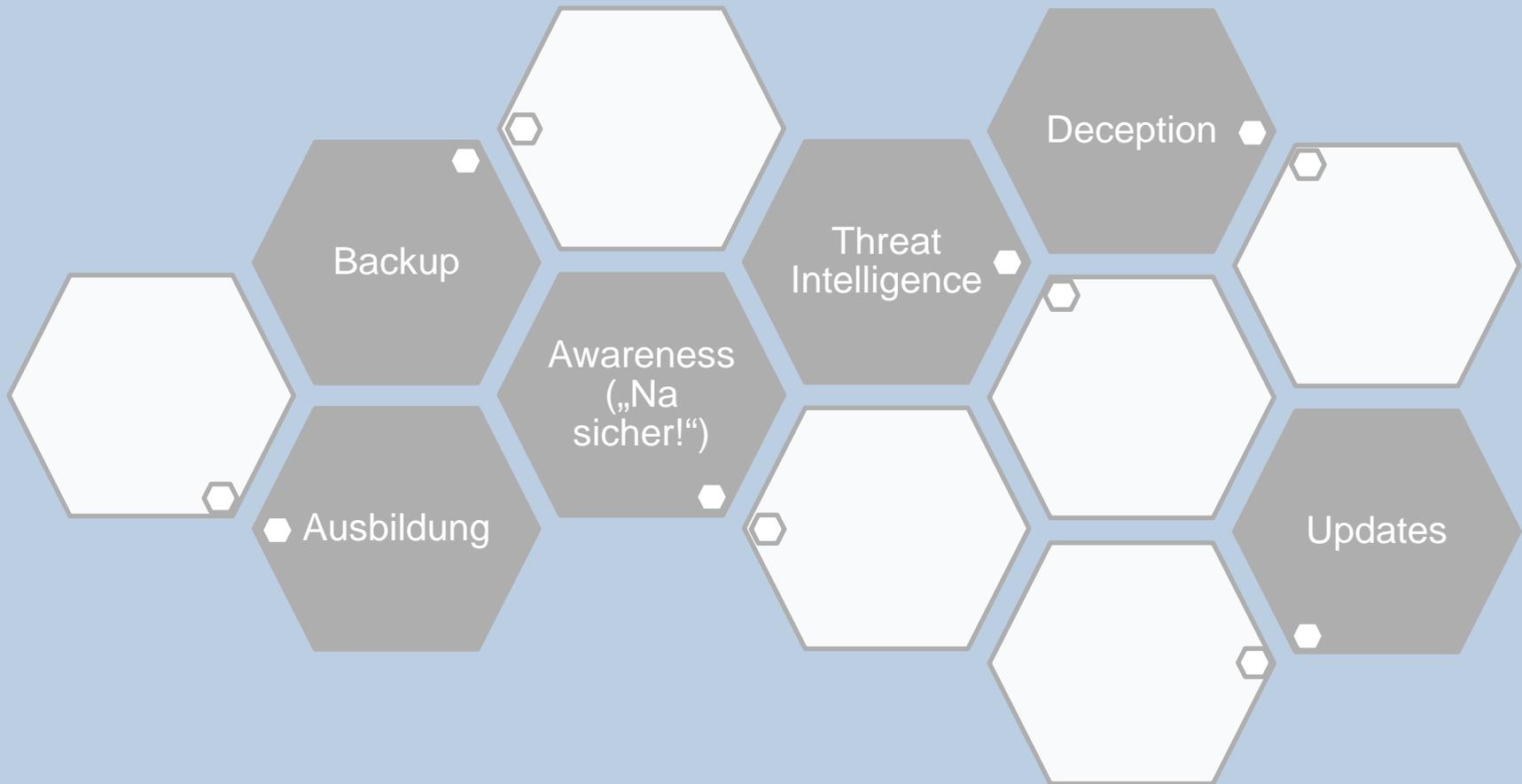


Reaktion





Prävention





Fazit

Wir machen es den Angreifern noch zu leicht.

Das wollen wir ändern.