



x2&C92ly7i
bxz5ep22:r



Cyber-Bedrohung in hoher Frequenz...

2.500 - 6.500 Angriffe auf Netze des Bundes täglich

4.353 Infektionen mit Schadsoftware (Clients) im 1. HJ 2015

ca. **1,8 Mio.** sicherheitsrelevante Ereignisse an Internetübergängen &

105.000 in Einsätzen im 1. HJ 2015

Hochwertdienststellen im Inland ca. **25.000** Ereignisse im 1. HJ 2015

...aber wirkliche Angriffe **anspruchsvoll und schwer erkennbar**

Ø 205 Tage bis zur **Erkennung** eines Einbruchs

Ø 32 weitere **Tage** bis zur **Lösung** des Problems

100 % der Opfer hatten **Firewalls** und **Anti-Virus** Signaturen



Cyber-Bedrohung unterscheidet sich von konventionellen Bedrohungen





Warum Cyber jetzt? Bundeswehr muss auf zwei Ebenen reagieren

Selbstschutz als Großorganisation

Bundeswehr zunehmend bedroht

- in Stäben / **Hauptquartieren**
- in **Waffensystemen**
- in der **Supply Chain**



Im Sinne des Auftrags von Streitkräften

Bedrohung **keine Sci-Fi**

- Ukraine Krise (2014)
- STUXNET (2010)
- Georgien Krise (2008)
- Estland (2007)

NATO/EU/VN/OSZE setzen sich derzeit **verstärkt mit Rolle Cyber-Verteidigung** auseinander



NATO hat in Wales **Cyber zum möglichen Bündnisfall** ausgerufen



Zwei parallele Ziele: Um, erstens, Cyber effektiver aufzustellen, muss, zweitens, auch die Bundeswehr-IT effektiver werden



Rolle des **Cyber- und Info-Raums als eigene Dimension stärken** und angemessen organisatorisch abzubilden

→ ("InfoRaum bündeln = Bw-IT ordnen")



Effektivität und Effizienz der Bundeswehr-IT zeitgemäß steigern

→ ("Bw-IT modernisieren")



Was hat die Bw bereits? Die Bundeswehr fängt nicht bei null an

IT Backend



Rechen- und Betriebszentren

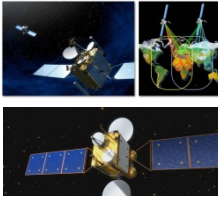
BtrbZ IT-SysBw
Rechenzentrum

Militärisches Frontend



IT in Waffensystemen

Militärische Satelliten




ComSatBw 1 + 2
Kommunikation

Heinrich Hertz



Computer Emergency Response Teams der Bw & BWI

BWI
www.bwi-it.de



Computer Netzwerk Operationen



TerraSAR / TanDEM-X
z.B. Geländeprofile

NAVSTAR GPS



Gefechtsstände



Funk Datenlink Krypto



SAR-Lupe -> SARah
z.B. optische Aufklärung

FRA HELIOS -> CSO

u.v.m.



Diagnose: IT- und Cyber-Fähigkeiten bereits operative vorhanden – aber ausbaufähig und zusammenzuführen



In Zukunft klare Cyber-Schnittstellen für Partner und andere Ressorts

