CYBER DEFENSE

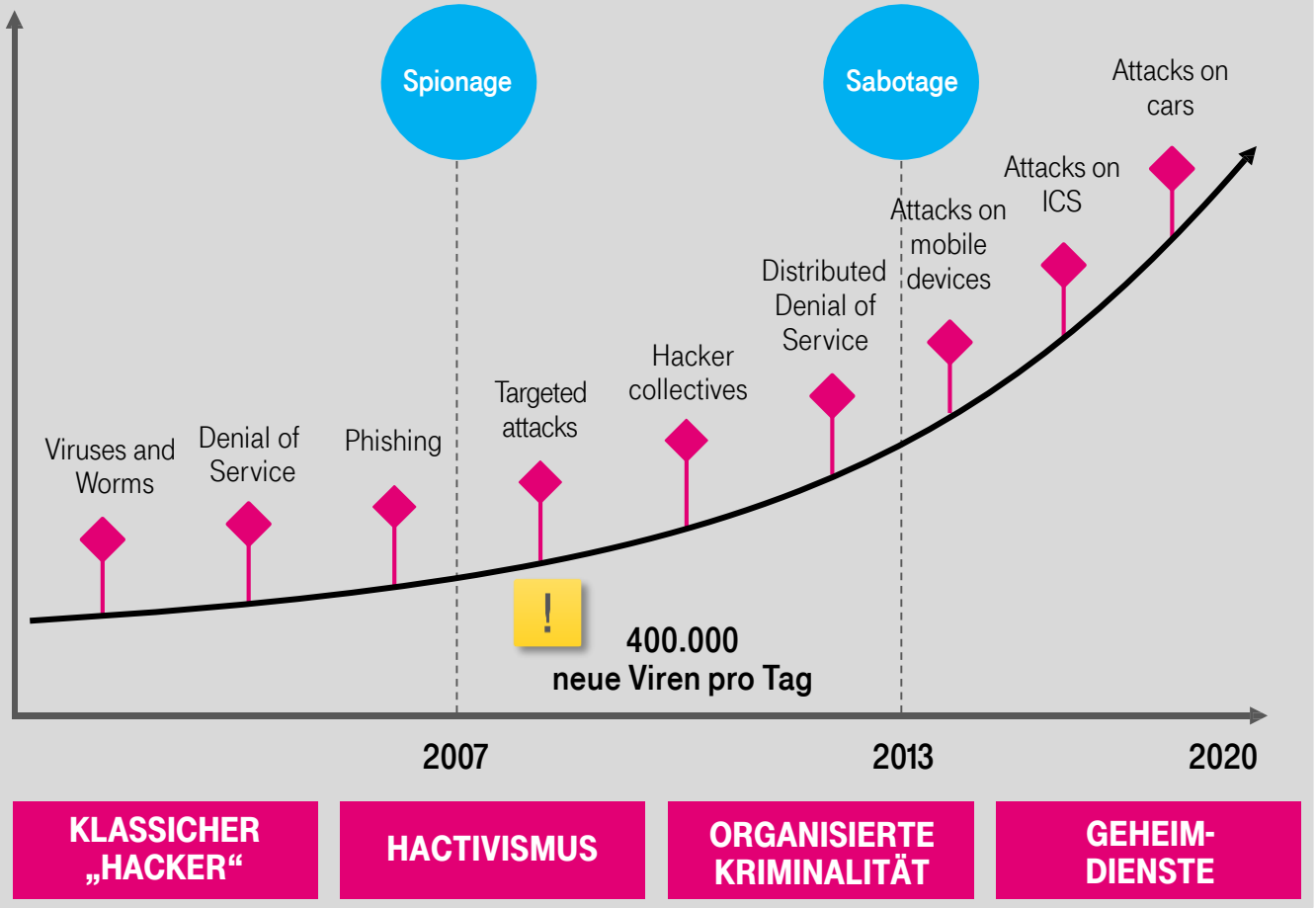
ZKI Frühjahrstagung 2016

Frankfurt (Oder), 8. März 2016

Dr. Bernd Eßer

GEZIELTE CYBER ANGRIFFE
PROFESSIONALISIERUNG DER ANGREIFER

„VOM HOBBY ZUR ORGANISIERTEN KRIMINALITÄT“



HOT TOPICS

GEZIELTE CYBER ANGRIFFE
TYPISCHE VORGEHENSWEISE DER TÄTER

EINDRINGEN

- Phishing Mails
- Drive-by-Exploits
- Antivirus erkennt die Schadsoftware nicht

LATERAL BEWEGUNG

- Pass-the-hash
- Pass-the-ticket
- Golden ticket

EXFILTRATION

- HTTPS Verkehr
- E-Mail
- Komplexe Protokolle wie bspw Shockwave

Die Werkzeuge der Täter:

- E-Mail zur Infiltration
- WWW zur Fernsteuerung und Exfiltration

GEZIELTE CYBER ANGRIFFE
KANN DAS EINDRINGEN SICHER VERHINDERT WERDEN?

EINDRINGEN → **LATERAL BEWEGUNG** → **EXFILTRATION**

- Phishing Mails
- Drive-by-Exploits
- Antivirus erkennt die Schadsoftware nicht

AWARENESS

- Awareness-Schulungen

! Ein Phishing-Angriff ist bereits erfolgreich, wenn nur ein Mitarbeiter „klickt“

ANTIVIRUS

- Anti-Viren Industrie benötigt circa 2 Monate zur Erkennung neuer Viren

! Zum Zeitpunkt der Infektion wird der Virenprüfer die Schadsoftware nicht detektieren

SPEED

- Sobald ein Mitarbeiter „klickt“, wird er mit einer Fernsteuerungs-Software infiziert

! Innerhalb von wenigen Minuten „springt“ der Täter zum nächsten Rechner

CYBER SECURITY STRATEGIE

NOTWENDIGE NEUE & KOMPLEXE FÄHIGKEITEN

PRÄVENTION

Lateralbewegung erschweren

- Pass-the-hash und Pass-the-ticket durch geeignete Windows-Administrations-Konzepte verhindern
- Active Directory und Domain Controller speziell sichern um Golden-Ticket zu verhindern

DETEKTION

Logdaten

- Schneller Zugang zu Logs
- Übertragungskapazitäten
- Logdaten von nachhaltig guter Qualität
- Sniper- / Mass-Scale-Forensik
- IoC Blockierungsprozesse

REAKTION

CERT / Hunter Team

- Aufbau von Fähigkeiten in Analyse, Ermittlung, Forensik, Reverse Engineering und Big Data Science
- Entwicklung und Aufbau notwendiger Tools und IT-Strukturen

CYBER SECURITY STRATEGIE

DIE GRUNDLAGEN EINER INTEGRIERTEN STRATEGIE

PERSPEKTIVE DES ANGREIFERS

- Cyber Crime generiert hohe Gewinnmargen
- Täter können in neue Werkzeuge und Vorgehensweisen investieren
- Strafverfolgungsrisiko ist niedrig

! Cyber Crime - Ein Wachstumsmarkt

PERSPEKTIVE DER INTERNEN SICHERHEIT

- Security ist üblicherweise „Cost of doing business“
- Cyber Security Exzellenz wird normalerweise nur wenig anerkannt bzw belohnt

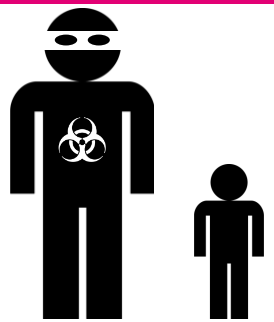
! Die Kluft zwischen Angreifer und Verteidiger wird größer

1. **“NUR ISMS” IST NICHT GENUG NEUE FÄHIGKEITEN SIND NOTWENDIG**
2. **SECURITY COST MANAGEMENT DURCH HARMONISIERUNG & STANDARDS**
3. **INVESTITIONEN IN DEN AUFBAU VON DETEKTION UND REAKTION**
4. **ZUSAMMENARBEIT UND AUSTAUSCH STÄRKEN DIE EIGENE POSITION**

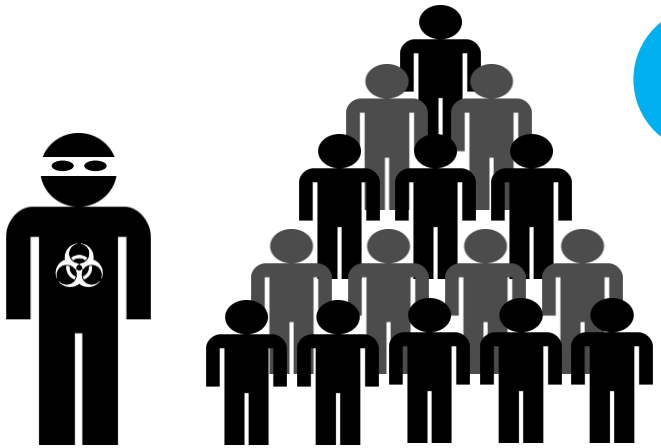
CYBER SECURITY STRATEGIE

KOLLABORATION – WICHTIGER HEBEL DER STRATEGIE

FROM



TO



1. **CYBER SECURITY NACHBARSCHAFTSHILFE**
2. **GEMEINSAME ENTWICKLUNG VON WERKZEUGEN UND METHODEN**
3. **CYBER BEDROHUNGS-LAGEBILD**

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!