



Information Security and Privacy

Modul D3.2 – Lecture 1.2

Referent: Dr. Jörg Cosfeld

Lecture 1.2 – Schutzziele der IT

Schutzziele der IT

- Gutes Verständnis für eigene Aspekte der IT Sicherheit
- Erlangen folgender Bausteine:
 - Idee
 - Aufbau
 - Konzept
- Folgende
 - Beispiele und ihre schematische Darstellung

Schutzziele der IT

- Wie ist die aktuelle Sicherheitslage?
 - Digitale Transformation auf allen Ebenen beschleunigt
 - Wertschöpfung der IT steigt in Hinsicht aller Produkte
 - Sicherheitsprobleme werden jedes Jahr größer
 - Heutige IT ist nicht sicher genug
 - Angreifer scheinen immer intelligenter zu sein?
- **Resultierende Herausforderungen:**
 - Infrastrukturen werden **immer komplexer**
 - Methoden der **Angreifer** werden **komplexer**
 - **Ziele** werden **lukrativer**

Schutzziele der IT

- **Risiken steigen** sehr stark an!
- Vorgänge wie:
 - Diebstahl
 - Spionage
 - Sabotage
- Aktuelle Lage ist
 - Ungenügend
 - Keine gute Basis



**Wirtschaftlicher Gesamtschaden
220 Milliarden Euro**

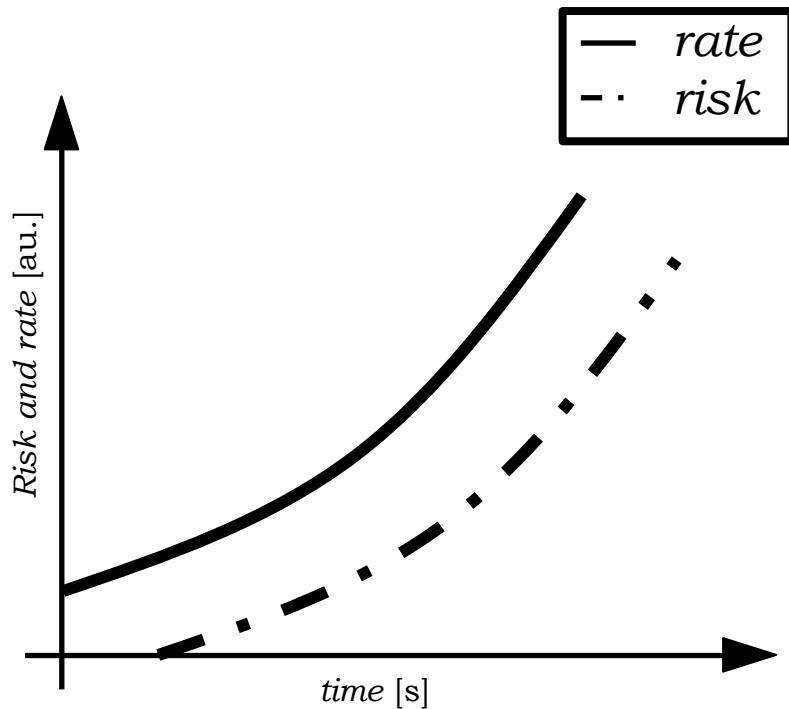
Schutzziele der IT

- **Risiken steigen** sehr stark an!
- Vorgänge wie:
 - Diebstahl
 - Spionage
 - Sabotage
- Aktuelle Lage ist
 - Ungenügend
 - Keine gute Basis



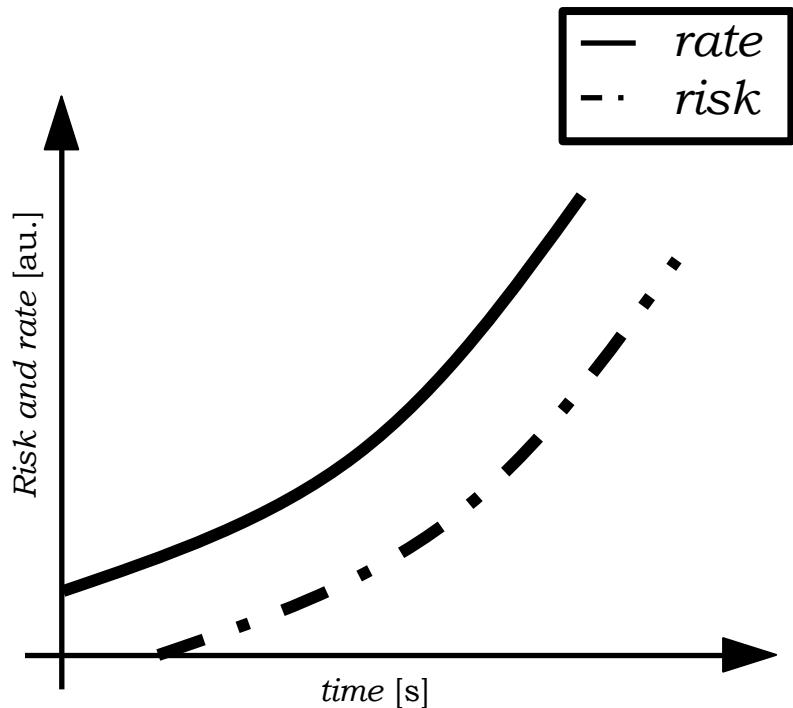
**Wirtschaftlicher Gesamtschaden
220 Milliarden Euro**

Schutzziele der IT



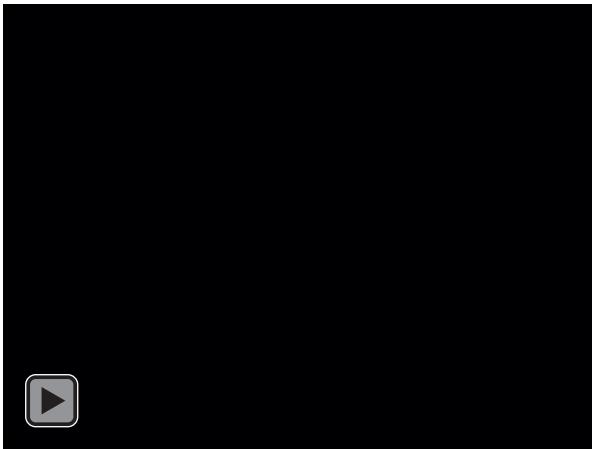
- Digitalisierung – Treiber
 - Kommunikation (5G, Glasfaser)
 - Smarte Endgeräte
 - Power der IT Systeme (Cloud, Hyperscaling, HPC)
 - AI – artificial intelligence
 - Fusion aus Prozess und Tool

Schutzziele der IT



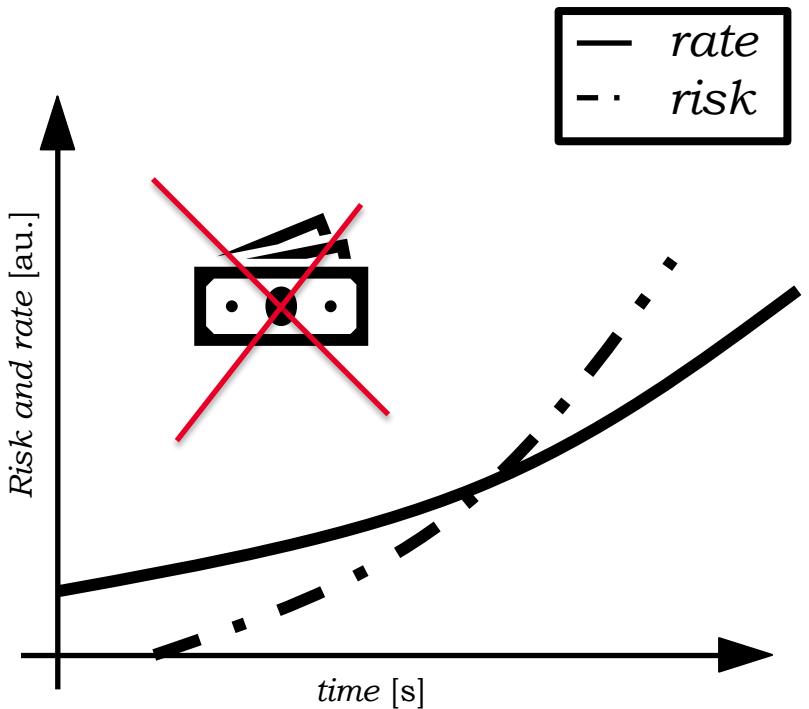
- Digitalisierung – **Treiber**
 - Kommunikation (5G, Glasfaser)
 - Smarte Endgeräte
 - Power der IT Systeme (Cloud, Hyperscaling, HPC)
 - AI – artificial intelligence
 - Fusion aus Prozess und Tool
- Digitalisierung – Bremser **Hürden**
 - Schlechte Softwarequalität
 - Mailverschlüsselungen (TLS)
 - Umgang mit komplexen Systemen
 - Angepasste Sicherheitsarchitektur
 - Sichere Hardware

Schutzziele der IT



- Digitalisierung – **Treiber**
 - Kommunikation (5G, Glasfaser)
 - Smarte Endgeräte
 - Power der IT Systeme (Cloud, Hyperscaling, HPC)
 - AI – artificial intelligence
 - Fusion aus Prozess und Tool
- Digitalisierung – Bremser **Hürden**
 - Schlechte Softwarequalität
 - Mailverschlüsselungen (TLS)
 - Umgang mit komplexen Systemen
 - Angepasste Sicherheitsarchitektur
 - Sichere **Hardware**

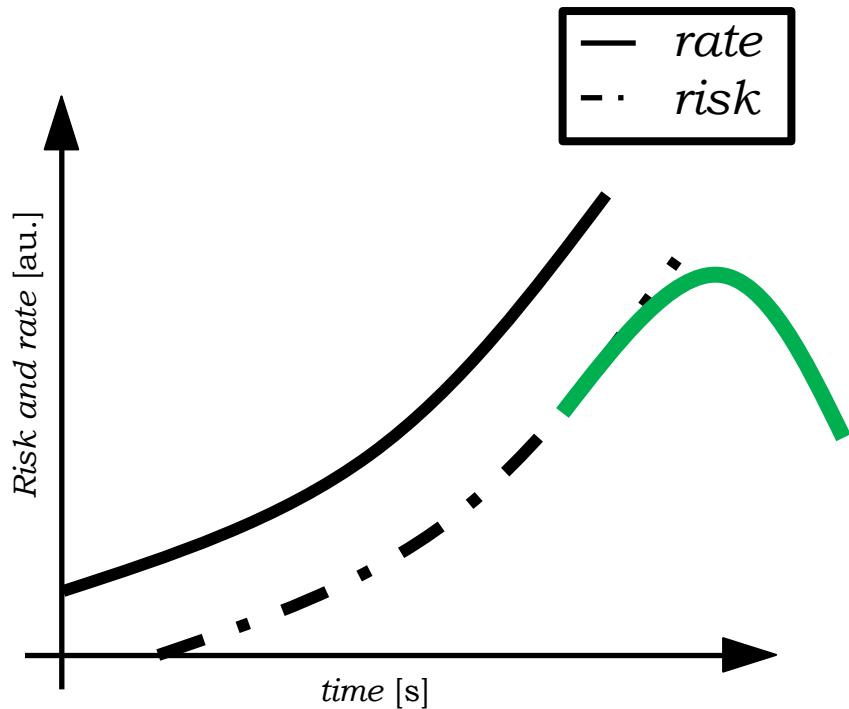
Schutzziele der IT



Kreuzung der
Kurven
=
Nicht Wirtschaftlich

- Digitalisierung – Bremser **Hürden**
 - Schlechte Softwarequalität
 - Mailverschlüsselungen (TLS)
 - Umgang mit komplexen Systemen
 - Angepasste Sicherheitsarchitektur
 - Sichere Hardware

Schutzziele der IT



- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Digitalisierung – Bremser **Hürden**
 - Schlechte Softwarequalität
 - Mailverschlüsselungen (TLS)
 - Umgang mit komplexen Systemen
 - Angepasste Sicherheitsarchitektur
 - Sichere Hardware

Vermeiden von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Definition:

Ein angestrebter Schutz von der Wirtschaftlichkeit eines Unternehmens ist die Idee Schaden zu vermeiden.

Vermeidungsstrategie

Vermeiden von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Definition:

Ein angestrebter Schutz von der Wirtschaftlichkeit eines Unternehmens ist die Idee Schaden zu vermeiden.

Vermeidungsstrategie

Beispiel: Autoreifen mit Pannenschutz



Vermeiden von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
- Voraussetzung:
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Beispiel: Autoreifen mit
Pannenschutz

Anwendung:

- **Datensparsamkeit**
- Nur so viele Daten wie nötig.
- Ablageort strategisch wählen

Vermeidungsstrategie



Vermeiden von Angriffen

- Abbau von Risiken
 - **Vermeiden von Angriffen**
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Beispiel: Autoreifen mit
Pannenschutz

Anwendung:

- **Verwendete Produkte / Dienste**
- Keine Produkte und Dienste mit Schwachstellen anwenden

Vermeidungsstrategie

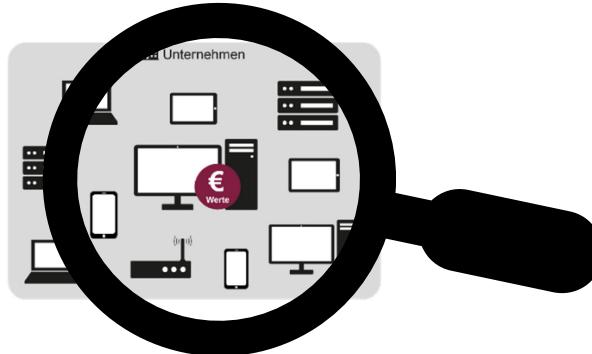


Vermeiden von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

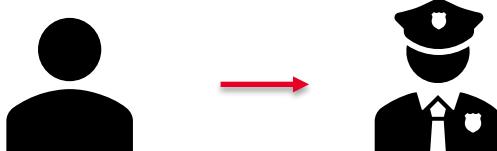
Anwendung:

- **Fokussierung**
- Was sind Daten von sehr hohen wirtschaftlichen Wert?
- **Schutzbedarfsanalyse**
 - Definition von Schutzbedürftigkeit



Vermeiden von Angriffen

- Abbau von Risiken
 - **Vermeiden von Angriffen**
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren



Anwendung:

- **Wert der Mitarbeiter**
- Sensibilisieren und Fortbilden
(Change Management)
- **Wissen der MA**
- **Einstellung der MA**
- Relevantes Wissen:
 - Werte des Unternehmens
 - **Organisatorischen
Regelungen**

Vermeiden von Angriffen

- Abbau von Risiken
 - **Vermeiden von Angriffen**
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Anwendung:

- **Datensparsamkeit**
- **Produkte / Dienste**
- **Fokussierung**
- **Wert der Mitarbeiter**

Schäden können vermieden werden.

Wenn Angriffsfläche reduziert wird und notwenige Systeme gesichert werden.

Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Definition:

Ein bereits vorhandenes Risiko muss minimiert werden.

Strategie zur Prävention

Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Anwendung:

- **Verschlüsselung** von Daten, Festplatten, TLS/SSL
- Schutz vor Dritten

**Strategie zur
Prävention**



Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Anwendung:

- **Multifaktor-Authentifikationsverfahren**
- Ausschluss von unbekannten aus dem System

**Strategie zur
Prävention**



Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Anwendung:

- **Anti Maleware Lösungen**
- Schutz vor Softwareinstallationen Dritter auf dem System

Strategie zur Prävention



Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Anwendung:

- **Anti DDoS Lösungen**
- Schutz vor DDoS Angriffen
 - DDoS Lecture 4

**Strategie zur
Prävention**



Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Anwendung:

- **Verwendung von Signaturen**
- Signaturverfahren schützen vor dem Vortäuschen von digitalen Handlungen.
Strategie zur Prävention



Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

Anwendung:

- **Hardware-Sicherheitsmodul**
- Klassische Firewall
- Unterbindung von unerlaubten Zugriffen auf das System.

**Strategie zur
Prävention**



Angriffen Entgegenwirken

- Abbau von Risiken
 - Vermeiden von Angriffen
 - **Prävention**
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren



Anwendungen:

- **Verschlüsselung**
- **Multifaktor-Authentifikationsverfahren**
- **Anti-Malware**
- **Anti DDoS**
- **Signaturen**
- **Hardware-Module**

Anwendungen müssen den Kurven folgen! Steht aber meistens nicht schnell genug zur Verfügung.

Erkennen von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- Angriff erkennen und Schaden minimieren
 - Man muss schneller sein als der Angreifer



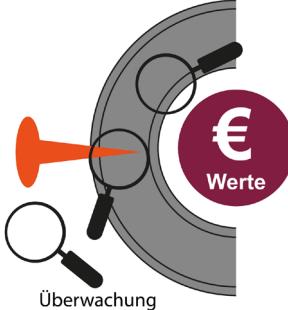
Erkennen von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- **Lagebilder** erstellen
 - **Warnungen** erzeugen
 - Windows hat spezielle Monitoring Tools für Server



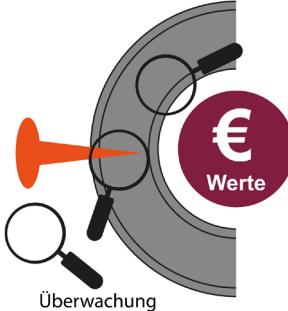
Erkennen von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- **Lagebilder** erstellen
 - **Warnungen** erzeugen
 - Windows hat spezielle Monitoring Tools für Server



Erkennen von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- **Lagebilder** erstellen
 - **Warnungen** erzeugen
 - Windows hat spezielle Monitoring Tools für Server
 - Ablauf am Besten definiert und automatisiert
 - Nur selten der Fall
 - **Keine 100%tige Erfolgsrate!**



Erkennen von Angriffen

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren

**Keine
100%tige
Schaden
Abdeckung /
Verhinderung**



Auf Angriffe aktiv reagieren

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- **Automatisierte Reaktion**
 - Setze Erkennung voraus
 - **Firewall Regeln**
 - **Angriffsfläche gering halten**



Auf Angriffe aktiv reagieren

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
- **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren



Anwendungen:

- **Definition von Befugnissen und Kommunikationsstrategien**
- Abschalten der Internetverbindung
- Kommunikationswege müssen klar sein
- Kurze Entscheidungsprozesse
- Kommunikationsstrategie
 - Wie werden MA informiert?
 - Wann?
- Imageschaden vermeiden

Auf Angriffe aktiv reagieren

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- **Digitale Forensik**
 - Analyse des Angriffes im Sinne der detaillierten Nachverfolgung
 - Zeigt Schwachstelle auf
 - Kann angewendet werden um verlorene Daten zu retten.



Auf Angriffe aktiv reagieren

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- **Notfallplanung**
 - Festlegen erprobter Reaktionskonzepte
 - Kann Nervosität nehmen
 - Reaktion kann trainiert werden



Auf Angriffe aktiv reagieren

- Abbau von Risiken
 - Vermeiden von Angriffen
 - Prävention
 - **Voraussetzung:**
 - Angriffe erkennbar machen
 - Auf Angriffe reagieren
- Anwendungen:
- Automatisierte Reaktion
 - Firewall Regeln
 - Angriffsfläche gering halten
 - Definition von Befugnissen und Kommunikationsstrategien
 - Digitale Forensik
 - Notfallplanung



Motivation der Angreifer

Was sind Motivationen und Zielbilder von Angreifern?



Ihre Ideen?

Motivation der Angreifer

Was sind Motivationen und Zielbilder von Angreifern?



- **Anerkennung**
 - Ruhm in der Community – Vergleich zu Graffiti Künstlern
- **Geld**
 - Erpresserische Angriffe setzen BitCoin Transfers als Ziel
 - IT Spione – Ransomware – Bitlocker
- **Herausforderung**
 - Hacker möchte selber lernen und erfährt eine Befriedigung
- **Neugierde**
 - Neugierde kann auch eine Form von Befriedigung sein

Motivation der Angreifer

Was sind Motivationen und Zielbilder von Angreifern?



- **Spaß**
 - Spaß an der Technik und daran neue Schlupflöcher zu finden
- **Zerstörungswut**
 - Angreifer greift an, weil er dem Unternehmen nicht gut gewonnen ist.
 - Oft ehemalige Mitarbeiter

Angreifer Typen

Definition:

- **Hacker**
 - Hacker brechen in Netzwerke (digital ein) und sehen ihren Erfolg als Statuszuwachs
 - Oft unprofessionell, auch Skript-Kiddies genannt
- **IT Spione**
 - Bezahlte Professionals, mit sehr hohen Budget, versuchen über Angriffe an Informationen zu kommen
 - Politische und wirtschaftliche Ziele.



Angreifer Typen

Definition:

- **Hacker**
 - Hacker brechen in Netzwerke (digital ein) und sehen ihren Erfolg als Statuszuwachs
 - Oft unprofessionell, auch Skript-Kiddies genannt
- **IT Spione**
 - Bezahlte Professionals, mit sehr hohen Budget, versuchen über Angriffe an Informationen zu kommen
 - Politische und wirtschaftliche Ziele.



US-Geheimdienste

Russland gab offenbar 300 Millionen Dollar für Wahleinmischung aus

Laut US-Medien hat Russland seit 2014 riesige Summen an politische Parteien in mehr als 24 Ländern gezahlt. Das geht aus einem neuen Bericht der US-Geheimdienste hervor.

[113 Kommentare](#)



Angreifer Typen

Definition:

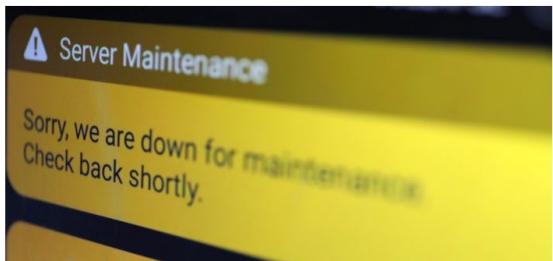
- **IT Terroristen**
 - Angst und Chaos sind das Ziel und die Motivation dieser Gruppe
 - Aufmerksamkeit auf Missstände und politische Ziele lenken
- **Unternehmens-Cracker**
 - Bezahlte Professionals die auf IT Systeme und Netzwerke der Konkurrenz zugreifen und wirtschaftliche Vorteile erzielen.
 - Spionage von Entwicklungsunterlagen, Pläne und Kundendaten



Angreifer Typen

Definition:

- **IT Terroristen**
 - Angst und Chaos sind das Ziel und die Motivation dieser Gruppe
 - Aufmerksamkeit auf Missstände und politische Ziele lenken



| Garmin offenbar down nach Hackangriff

9

Von Jörg Schieb am 25.07.2020



But Garmin successfully managed to pay off the criminals, using another intermediary on 24 or 25 July 2020, reported IT media outlets last weekend. The criminals then provided a WastedLocker decryption key to Garmin.

Angreifer Typen

Definition:

- **IT Terroristen**
 - Angst und Chaos sind das Ziel und die Motivation dieser Gruppe
 - Aufmerksamkeit auf Missstände und politische Ziele lenken



Düsseldorf

ZEIT^{ONLINE}

Ermittlungen zu Hackerangriff auf Uniklinik führen nach Russland

Vor zwei Wochen attackierten Hacker die Düsseldorfer Uniklinik – wohl unabsichtlich, aber mit womöglich tödlichen Folgen. Die Software kommt den Ermittlern bekannt vor.

Die Düsseldorfer Polizei habe dann tatsächlich Kontakt aufgenommen und den Tätern mitgeteilt, dass durch ihren Hackerangriff ein Krankenhaus – und nicht die Uni – betroffen sei, hieß es. Damit seien Patienten erheblich gefährdet. Die Täter hätten daraufhin die Erpressung zurückgezogen und einen digitalen Schlüssel ausgehändigt, mit dem die Daten wieder entschlüsselt werden können.

Angreifer Typen

Definition:

- **IT Terroristen**
 - Angst und Chaos sind das Ziel und die Motivation dieser Gruppe
 - Aufmerksamkeit auf Missstände und politische Ziele lenken



Düsseldorf

ZEIT^{ONLINE}

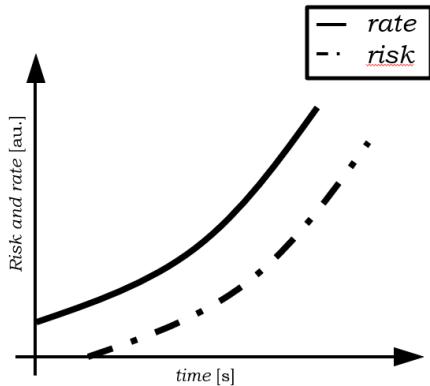
Ermittlungen zu Hackerangriff auf Uniklinik führen nach Russland

Vor zwei Wochen attackierten Hacker die Düsseldorfer Uniklinik – wohl unabsichtlich, aber mit womöglich tödlichen Folgen. Die Software kommt den Ermittlern bekannt vor.

„Deshalb stocken wir das Personal der NRW-Polizei im Bereich Cybercrime weiter auf“, sagte Innenminister Ralf Jäger. 36 IT-Fachleute werden das Cyber-Kompetenzzentrum im Landeskriminalamt mit zusätzlichem Knowhow verstärken.

Innenminister Ralf Jäger – 2017 – land.nrw.de

Angreifer Typen



Düsseldorf

ZEIT
ONLINE

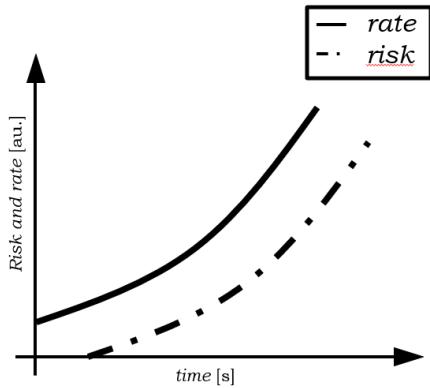
Ermittlungen zu Hackerangriff auf Uniklinik führen nach Russland

Vor zwei Wochen attackierten Hacker die Düsseldorfer Uniklinik – wohl unabsichtlich, aber mit womöglich tödlichen Folgen. Die Software kommt den Ermittlern bekannt vor.

„Deshalb stocken wir das Personal der NRW-Polizei im Bereich Cybercrime weiter auf“, sagte Innenminister Ralf Jäger. 36 IT-Fachleute werden das Cyber-Kompetenzzentrum im Landeskriminalamt mit zusätzlichem Knowhow verstärken.

Innenminister Ralf Jäger – 2017 – land.nrw.de

Angreifer Typen



Düsseldorf

ZEIT
ONLINE

Ermittlungen zu Hackerangriff auf Uniklinik führen nach Russland

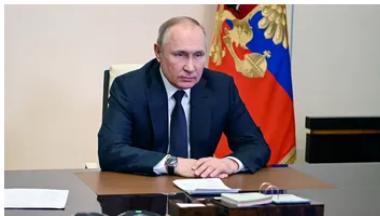
Vor zwei Wochen attackierten Hacker die Düsseldorfer Uniklinik – wohl unabsichtlich, aber mit womöglich tödlichen Folgen. Die Software kommt den Ermittlern bekannt vor.

Rund 0.4 mio Euro

„Deshalb stocken wir das Personal der NRW-Polizei im Bereich Cybercrime weiter auf“, sagte Innenminister Ralf Jäger. 36 IT-Fachleute werden das Cyber-Kompetenzzentrum im Landeskriminalamt mit zusätzlichem Knowhow verstärken.

Innenminister Ralf Jäger – 2017 – land.nrw.de

Angreifer Typen

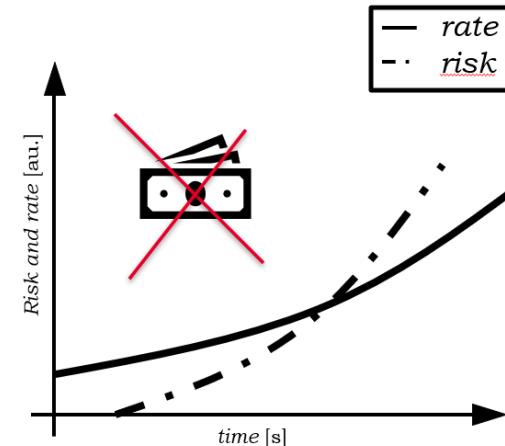


US-Geheimdienste

Russland gab offenbar **300 Millionen** Dollar für Wahleinmischung aus

Laut US-Medien hat Russland seit 2014 riesige Summen an politische Parteien in mehr als 24 Ländern gezahlt. Das gehe aus einem neuen Bericht der US-Geheimdienste hervor.

[113 Kommentare](#)



Rund 0.4 mio Euro

Düsseldorf

ZEIT^{ONLINE}

Ermittlungen zu Hackerangriff auf Uniklinik führen nach Russland

Vor zwei Wochen attackierten Hacker die Düsseldorfer Uniklinik – wohl unabsichtlich, aber mit womöglich tödlichen Folgen. Die Software kommt den Ermittlern bekannt vor.

„Deshalb stocken wir das Personal der NRW-Polizei im Bereich Cybercrime weiter auf“, sagte Innenminister Ralf Jäger. 36 IT-Fachleute werden das Cyber-Kompetenzzentrum im Landeskriminalamt mit zusätzlichem Knowhow verstärken.

Innenminister Ralf Jäger – 2017 – land.nrw.de

Angreifer Typen

Definition:

- **Professionelle Kriminelle – Gruppen**
 - Gruppe von Personen die sich persönlich bereichern wollen. Keine bezahlte Dienstleistung sondern erpresserischer Hintergrund
- **Vandalen**
 - Personen die einen Angriff durchführen nur um Schaden zu erzeugen.
 - Reine Zerstörungswut



Angreifer Typen



Definition:

- **Penetration Tester**
 - Experten die einen Penetration Test auf die Strukturen eines Unternehmens ausführen.
 - Kann Schwachstellen offenlegen und Angriffe erkennbar machen
- **Behördliche Mitarbeiter**
 - LKA – BKA Beamte
 - Einsatz des Know-Hows zur Verfolgung

Angriffsvektoren

Definition:

- Ein **Angriffsvektor** bezeichnet sowohl den **Weg** des Angriffes als auch die verwendete **Technik**.
- Angriffsweg kann mehrstufig oder verteilt sein
- Hierzu werden folgende Wege oft verwendet:
 - **Schwachstellen im Netzwerk**
 - **Social Engineering der Nutzer**
 - **Maleware**
 - **Exploits – Log4J**
 - **Brute Force**
- Installation von Keyloggern oder Ransomware



Angriffsvektoren

Definition:

- Ein **Angriffsvektor** bezeichnet sowohl den **Weg** des Angriffes als auch die verwendete **Technik**.
- Angriffsweg kann mehrstufig oder verteilt sein
- Hierzu werden folgende Wege oft verwendet:
 - **Schwachstellen im Netzwerk**
 - **Social Engineering der Nutzer**
 - **Maleware**
 - **Exploits – Log4J**
 - **Brute Force**
- Installation von Keyloggern oder Ransomware

Angriffsvektoren sind Hürdentreiber!

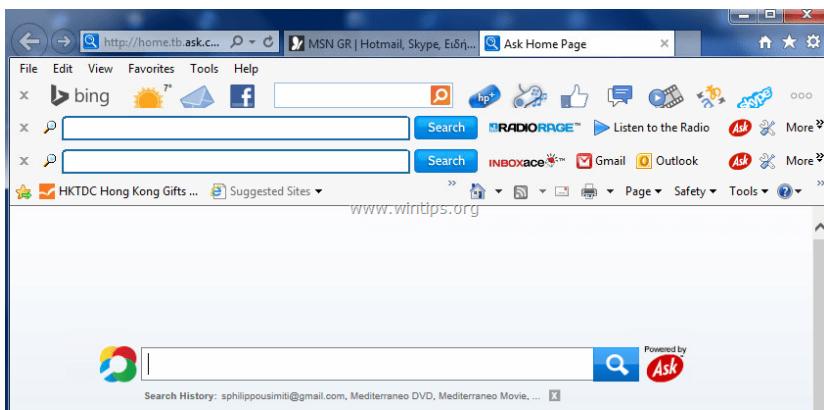


Angriffsvektoren – einige Beispiele

Installation einer Maleware über eine manipulierte Website

Drive-by Downloads

Maleware wird durch das vorbeigehen installiert.



Angriffsvektoren – einige Beispiele

Installation einer Maleware über eine manipulierte Website

Drive-by Downloads

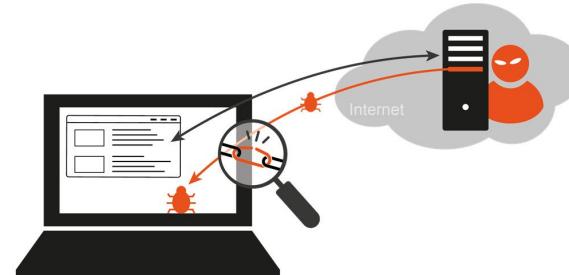
Maleware wird durch das vorbeigehen installiert.



Opfer wird zum Besuch der manipulierten Website motiviert.

Klassischer Phishing Versuch.

Drive-by Lücken werden dann ausgenutzt um spezielle Schadfunktionen zu nutzen.



Angriffsvektoren – einige Beispiele

Installation einer Maleware über Mailanhänge

Berufnetzwerk wird studiert und potenzielle Opfer werden analysiert.

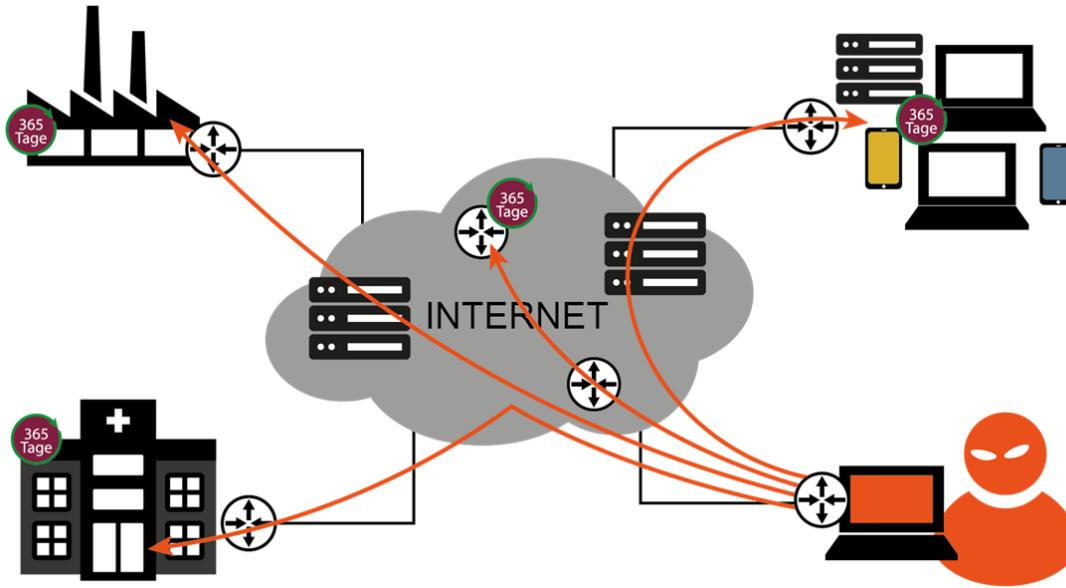
Kenntnisse werden genutzt um Opfern persönliche Nachrichten zu senden.

Klicken auf einen Anhang startet einen Prozess zur Installation einer Maleware.

Übernahme ist umgesetzt.

Angriffsvektoren – einige Beispiele

Installation einer Maleware über Mailanhänge



Angriffsvektoren – einige Beispiele

Man in the Middle Attack

- Einschleusen Dritter in das Zielsystem.
 - Zwischen mehrere Kommunikationspartner
- Logisch oder Physisch
- Kommunikationspartner nehmen an eine private Leitung zu haben.

Angriffsvektoren – einige Beispiele

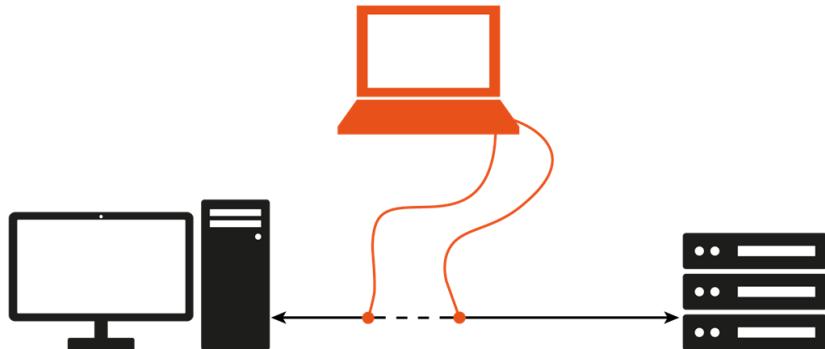
Man in the Middle Attack

- Einschleusen Dritter in das Zielsystem.
 - Zwischen mehrere Kommunikationspartner
 - Logisch oder Physisch
 - Kommunikationspartner nehmen an eine private Leitung zu haben.
- 

Angriffsvektoren – einige Beispiele

Man in the Middle Attack

- Einschleusen Dritter in das Zielsystem.
 - Zwischen mehrere Kommunikationspartner
- Logisch oder Physisch
- Kommunikationspartner nehmen an eine private Leitung zu haben.

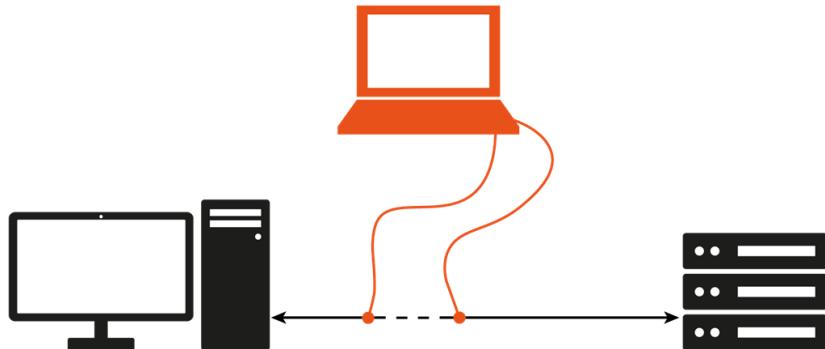


- Passwörter oder weitere / andere Daten können mitgelesen werden
- Daten können on the fly manipuliert werden

Angriffsvektoren – einige Beispiele

Man in the Middle Attack

- Einschleusen Dritter in das Zielsystem.
 - Zwischen mehrere Kommunikationspartner
- Logisch oder Physisch
- Kommunikationspartner nehmen an eine private Leitung zu haben.



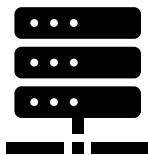
- Passwörter oder weitere / andere Daten können mitgelesen werden
- Daten können on the fly manipuliert werden

Angriffsvektoren – einige Beispiele

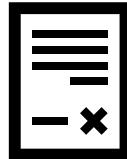
Supply Chain – Angriff

- Eine Supply Chain Angriff fokussiert sich auf das Eindringen in einen vertrauenswürdigen Dienst, der im Unternehmen etabliert ist.
 - Beispiel – Datenbanken
- Kompromittierte Software bekommt manipulierte Updates
 - Backdoor für den Angriff ist geschaffen

Kompromittierte Software



1. Supply



2. Signiertes Update

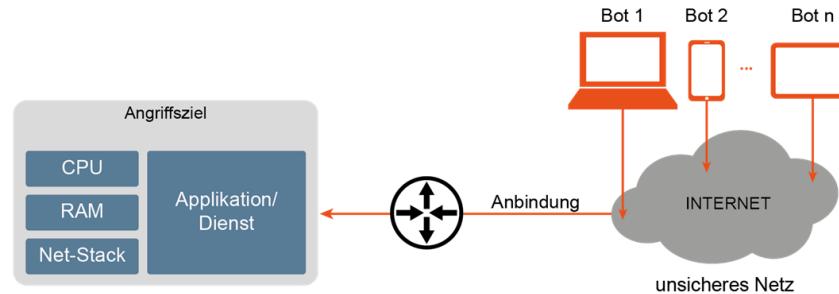


3. User

Angriffsvektoren – einige Beispiele

DDoS Angriff

- IT Systeme haben nur begrenzte Ressourcen
 - Bandbreite, CPU, RAM etc.
- IT System wird gezielt mit einer Fülle an Anfragen an Grenze gebracht
 - Hohe Last entsteht in allen Kanälen
 - System wird lahmgelegt
- Einsatz von Botnetzen – Schadfunktion **DDoS** wird aktiviert

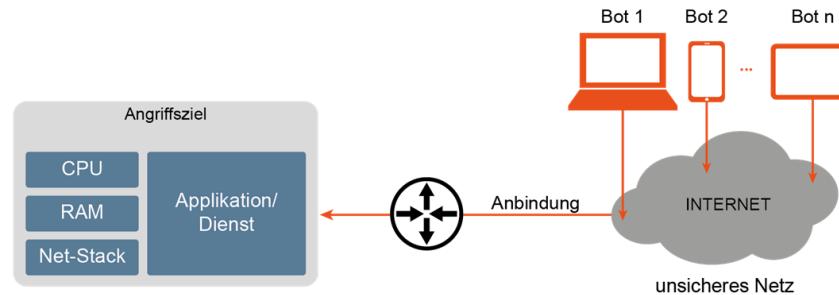


Angriffsvektoren – einige Beispiele

DDoS Angriff

Motivation:

- Wettbewerber soll lahm gelegt werden
- Erpresserische Absicht
 - Erst nach Zahlung wird die Attacke gestoppt

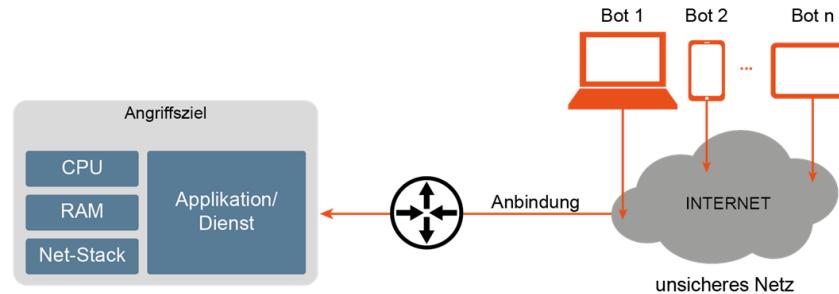


Angriffsvektoren – einige Beispiele

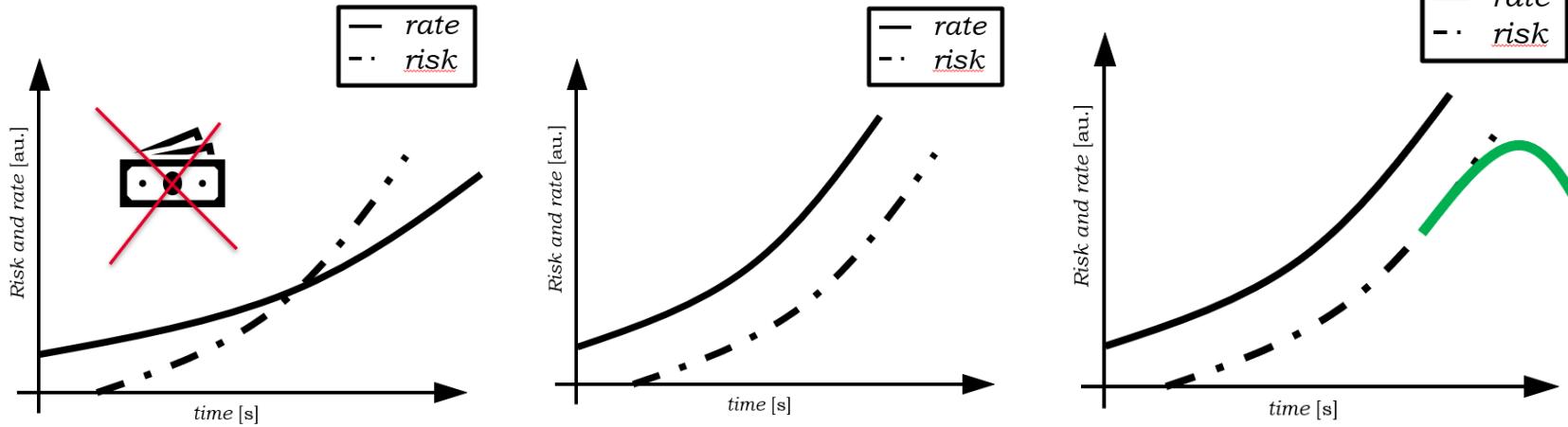
DDoS Angriff

Motivation:

- Wettbewerber soll lahm gelegt werden
- Erpresserische Absicht
 - Erst nach Zahlung wird die Attacke gestoppt



Rückblick



Rückblick

