Ministerium des Innern
des Landes Nordrhein-Westfalen

POLIZEI
Nordrhein-Westfalen

Cybercrime-Prävention

Präventive Polizeiarbeit im digitalen Raum

Inhalte
Grundlage, Arbeitsumfeld, Tätigkeit

Was bedeutet Prävention	Digitales Umfeld 2021	Polizeiarbeit 4.0
Verbrechen verhindern, bevor sie geschehen.	Das Internet: Milliarden vernetzte und kommunizierende Geräte	Beratung im und über den digitalen Raum.

Polizeiliche Präventionsarbeit

Im nächsten Abschnitt befindet sich die gesetzliche Grundlage für die polizeiliche Präventionsarbeit und dessen Ziel.

Zitat Erlass
- 42 - 62.02.01 vom 09. Mai 2019

Ziel polizeilicher, kriminalpräventiver Maßnahmen ist es, Bürger*innen, Wirtschaft, Verbände, öffentliche Verwaltung und andere Aufgabenträger zu sicherheitsbewusstem Verhalten zu veranlassen sowie potentielle Täter*innen der Begehung von Straftaten abzuhalten und so die Anzahl von Straftaten und Opfern zu verringern.

Die Polizei informiert insbesondere über Erscheinungsformen der Kriminalität, polizeiliche Bekämpfungsziele, Gefährdungseinschätzungen, Opferrisiken sowie tatbegünstigendes Verhalten. Sie gibt Empfehlungen zu tatreduzierenden Verhaltensweisen …

Cybercrime Prävention

Ist die proaktive Erarbeitung von Maßnahmen zur Abwendung und Vorbeugung von gegenwärtiger und zukünftiger Computer & Internetkriminalität mit der anschließenden Kommunikation dieser Maßnahmen an Büger*innen, KMU´s und andere Interessengemeinschaften.

Dies geschieht auf Basis von Ermittlungsergebnissen sowie aktuellen Studien und wissenschaftlichen Erkenntnissen.

Cybercrime Prävention

Ziel: Vor die Lage zu kommen

Wie kann die Lage zukünftig sein?

Die Lage wahrnehmen & verstehen

Warum ist die Lage, wie sie ist?

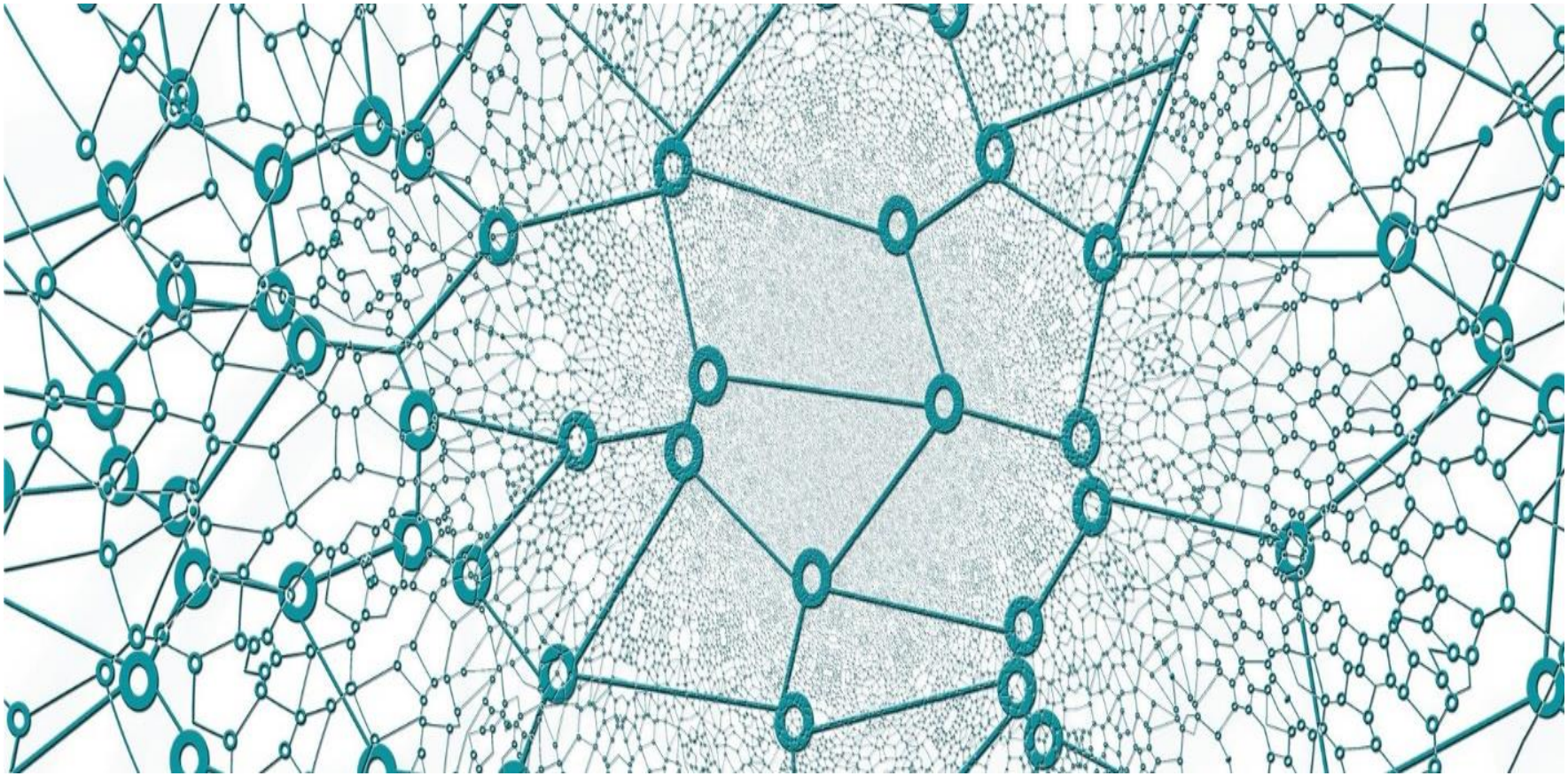
Die vergangene und aktuelle Lage analysieren

Wie ist die Lage?

Digitales Umfeld 2020 / 2021

Im nächsten Abschnitt werden Zahlen zu dem existierenden digitalen Umfeld geliefert.

Vernetzte Geräte 2020/2021



Vernetzte Geräte 2020/2021

2020: ca. 30 Mrd. vernetzte Geräte

2025: ca. 75 Mrd. vernetzte Geräte

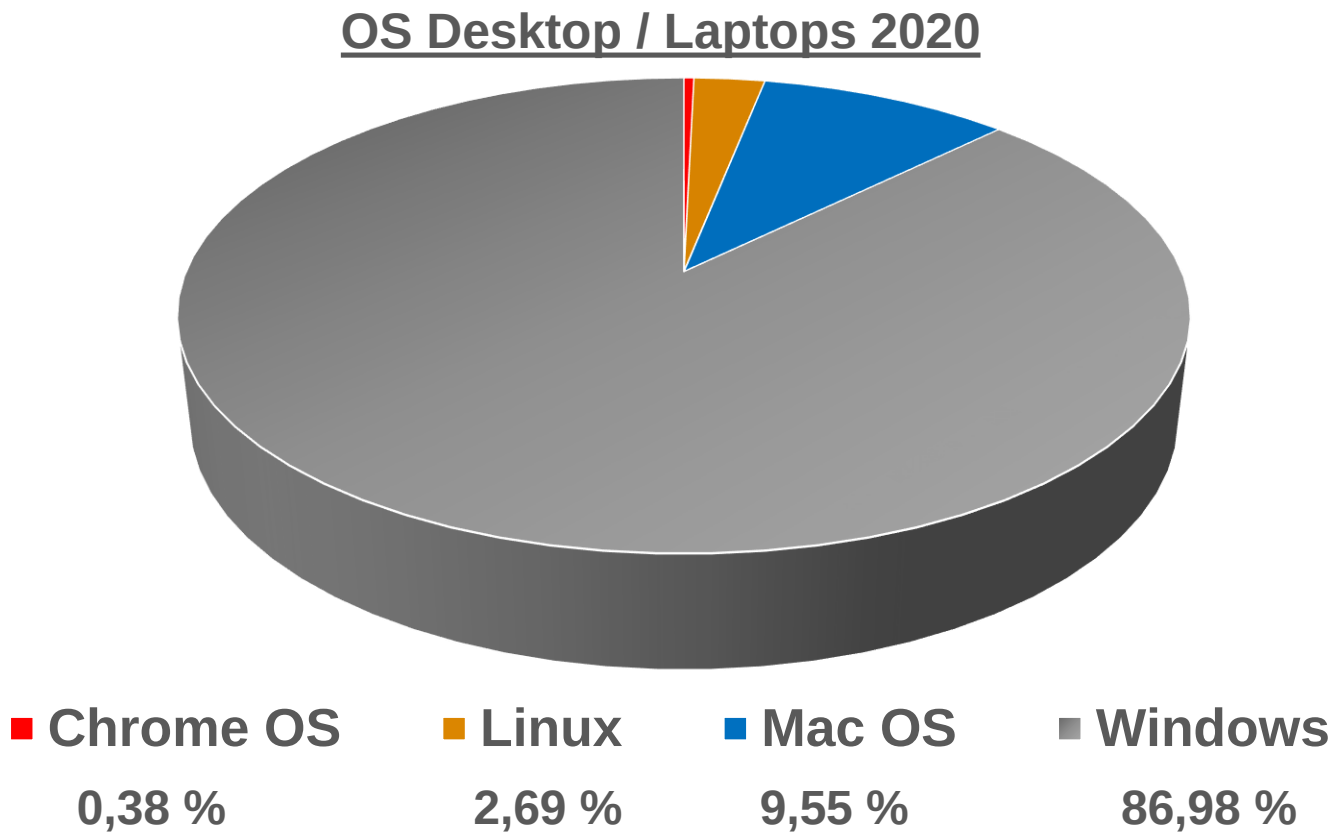
Datenquellen und –generierung

Datenquellen und –generierung

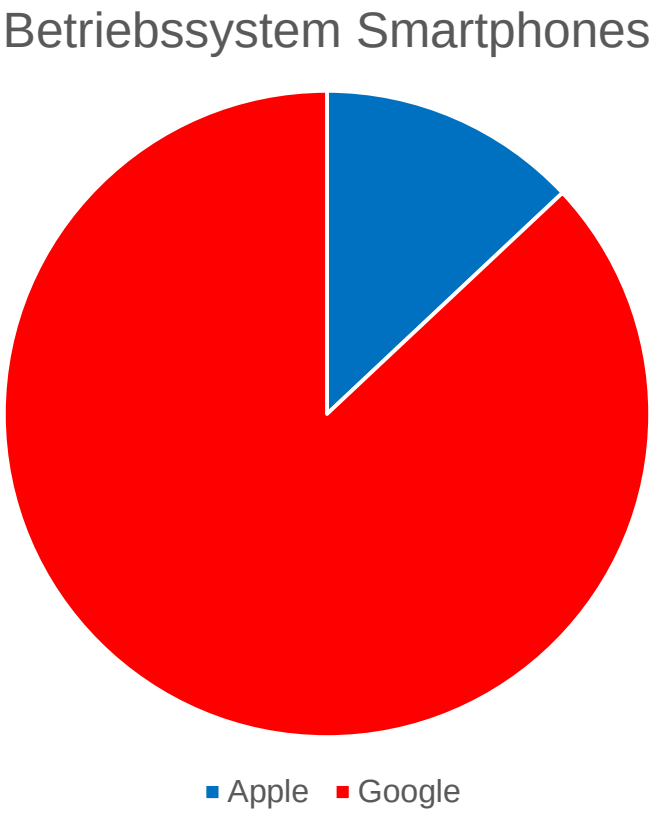
7,7 Mrd. Menschen Weltbevölkerung

Facebook / WhatsApp / Instagram	**2017**	→	4 Mrd.	**52%**
2 Mrd. / 1,2 Mrd. / 800 Mio				
Google+ Accounts	**2017**	→	3,36 Mrd.	**44%**
G-Pay – 5% d. Google Nutzer		→	168 Mio.	**2%**
Microsoft Geräte	**2017**	→	1,5 Mrd.	**20%**
Apple Unique User	**2017**	→	664 Mio.	**8%**
Apple Pay		→	253 Mio.	**2%**
Amazon Accounts	**2017**	→	300 Mio.	**3%**
Paypal 02/2020		→	346 Mio.	**4%**

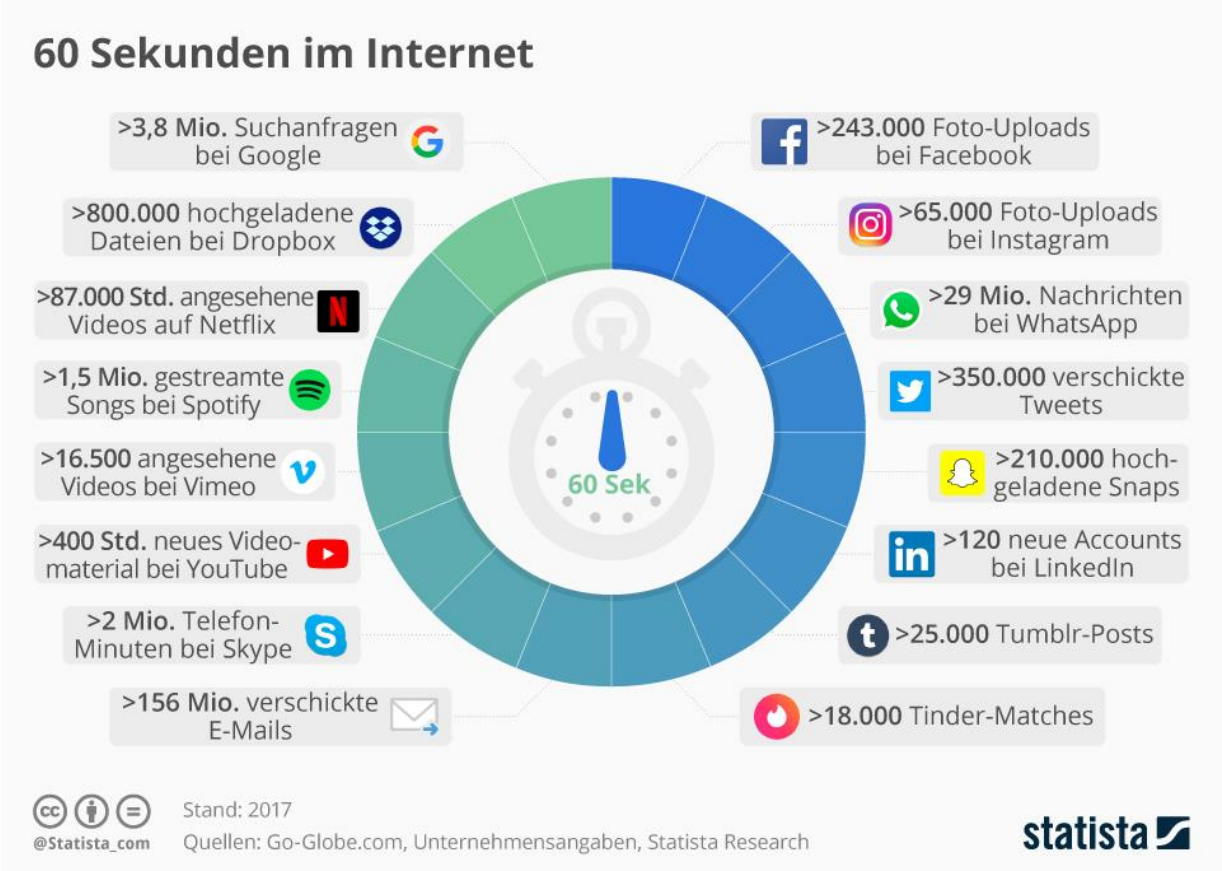
Datenquellen & -generierung



Datenquellen & -generierung



Generierte Daten in 60 Sekunden Internet



Datenquellen & -generierung

Polizeiarbeit 4.0

Im nächsten Abschnitt werden Informationen zu den derzeit gängigen Modus Operandi und den daraus abgeleiteten Vorgehen präsentiert.

Modus Operandi

ca. 59 % - 91 %

der Cyberattacken erfolgen per Mail

PWC Cyberangriffe gegen Unternehmen in Deutschland / Fireeye Studie 2019

Modus Operandi

ca. 30 %

der sicherheitskritischen Vorfälle sind auf „menschliches Versagen“, „Irrtum“ oder „Sabotage“ zurückzuführen

(Kaspersky Lab Global IT Risk Report)

Modus Operandi

Social Engineering als eine der beliebtesten Methode

(Proofpoint Studie 2019)

Modus Operandi

Studie Universität Bern (Januar 2020) Wirtschaftsspionage:
„In über 40% der Angriffe, also bei knapp der Hälfte der entdeckten Fälle, waren ehemalige (25%) oder aktuelle Mitarbeitende (16.7%) des Unternehmens involviert „

Schaden Cybercrime

13% der befragten Unternehmen hatten kürzlich einen **schweren** IT Sicherheitsvorfall (TÜV Cybersecurity Studie 2019)

75 % der Unternehmen waren in den vergangenen beiden Jahren von Angriffen betroffen (Bitkom 2019)

46 Mio. Cyberattacken pro Tag (Dt. Telekom 2019)

Schaden Cybercrime

100 Mrd. Euro in DE

(Bitkom)

Warum Cybercrime

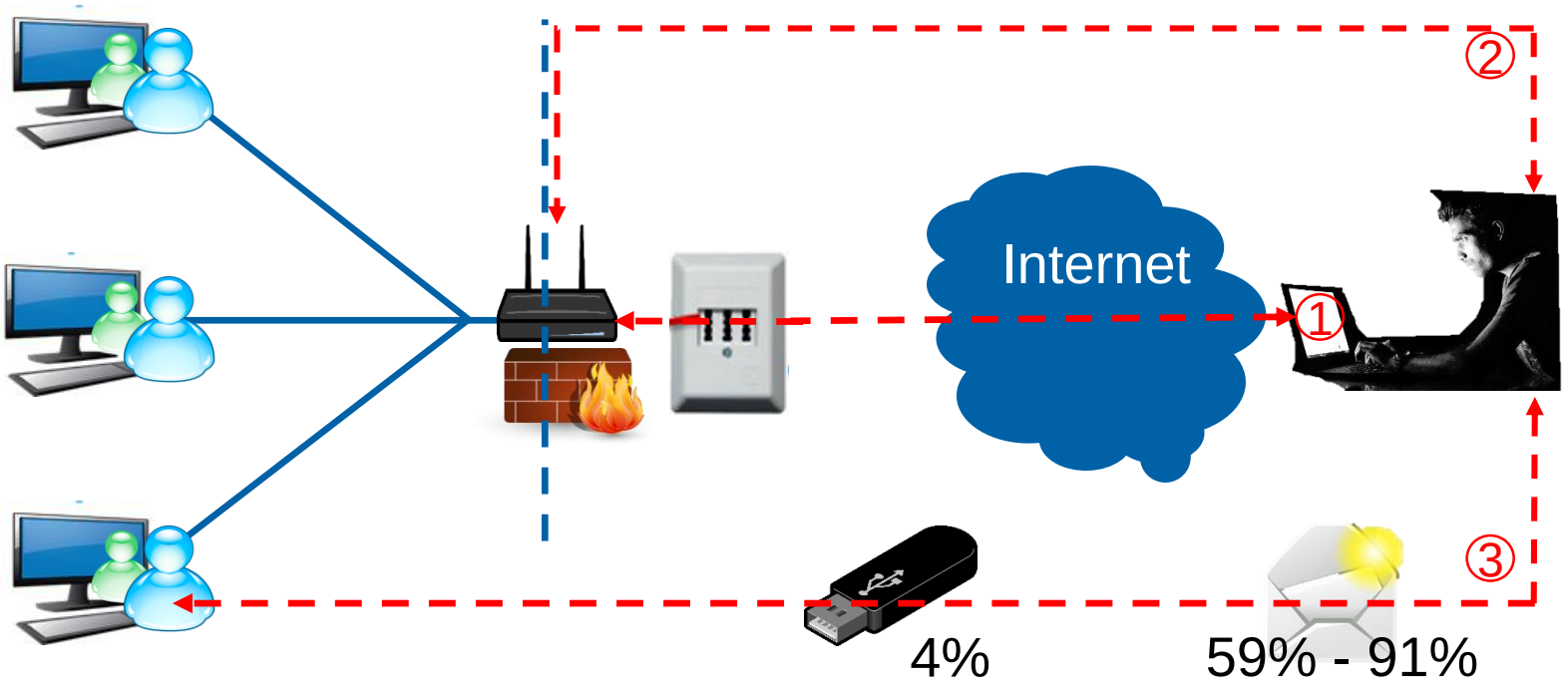
!!! Weil es so einfach und dabei auch noch günstig ist !!!

klassische „BWL-Frage“: Make or Buy?!
(Cyber)Crime as a Service

Ursache und das größte Problem an Cybercrime

„ist der Mensch“

Ursache und das größte Problem an Cybercrime



Ursache und das größte Problem an Cybercrime

„Wenn Du glaubst, dass Technologie [allein] deine Sicherheitsprobleme lösen kann, dann verstehst du die Probleme und Technologie nicht“

Zitate aus: Secrets & Lies, Bruce Schneier

Lösung für Cybercrime

Verhaltensprävention

Hat nebenher gesagt, auch das bessere
Kosten- / Nutzenverhältnis

Lösung für Cybercrime

Regel No.1

kritisch sein:  **AN**

neugierig sein:  **AUS**

Lösung für Cybercrime

Regel No.2

halte alle deine Systeme auf dem aktuellen Stand – Update, Update, Update

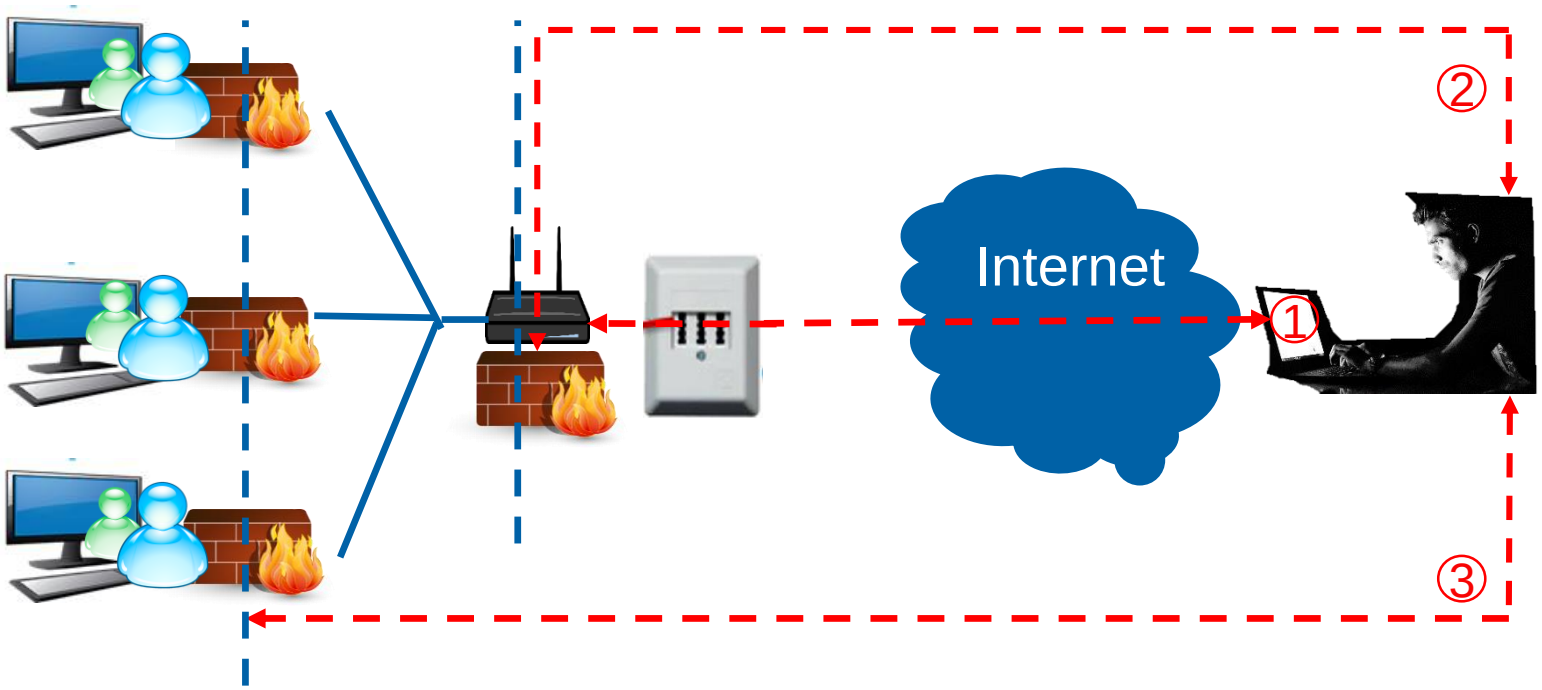
Lösung für Cybercrime

Regel No. 3

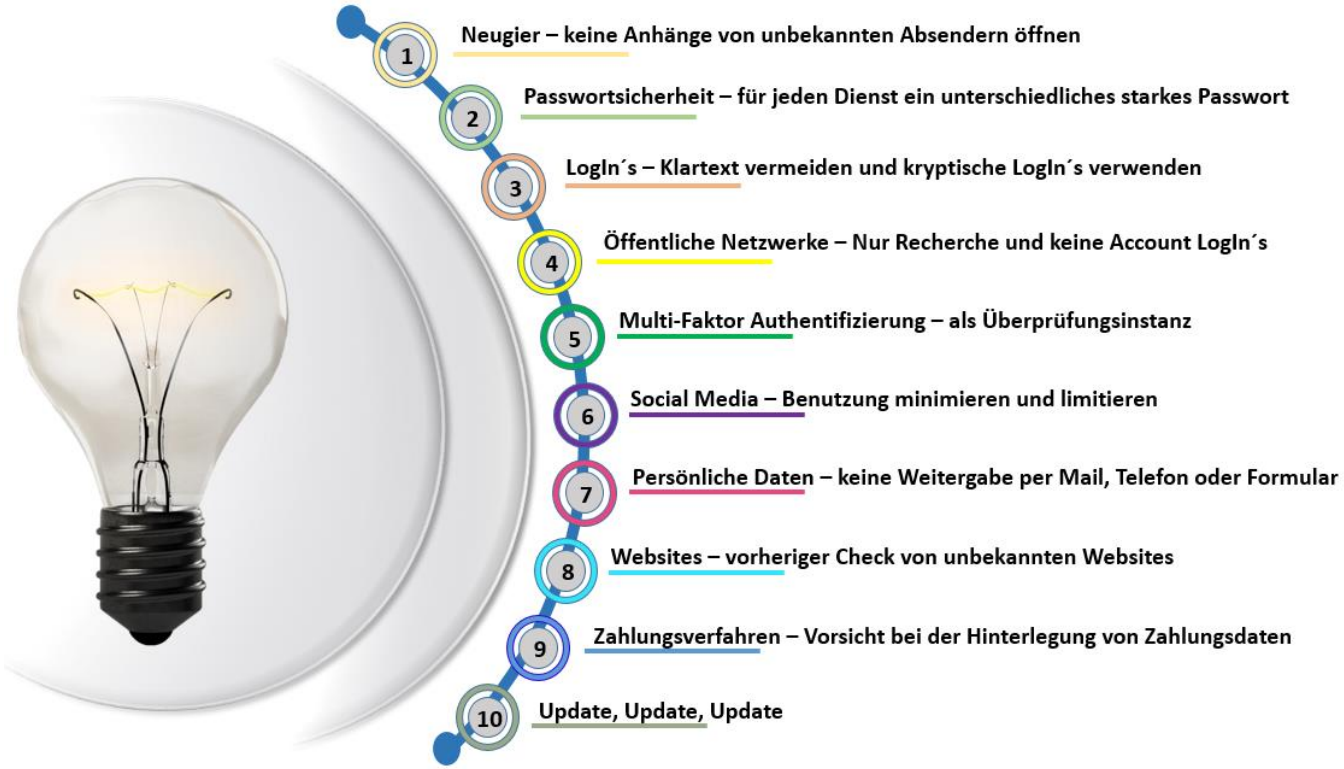
starke Passwörter

Lösung für Cybercrime

Lösung für Cybercrime



Lösung für Cybercrime

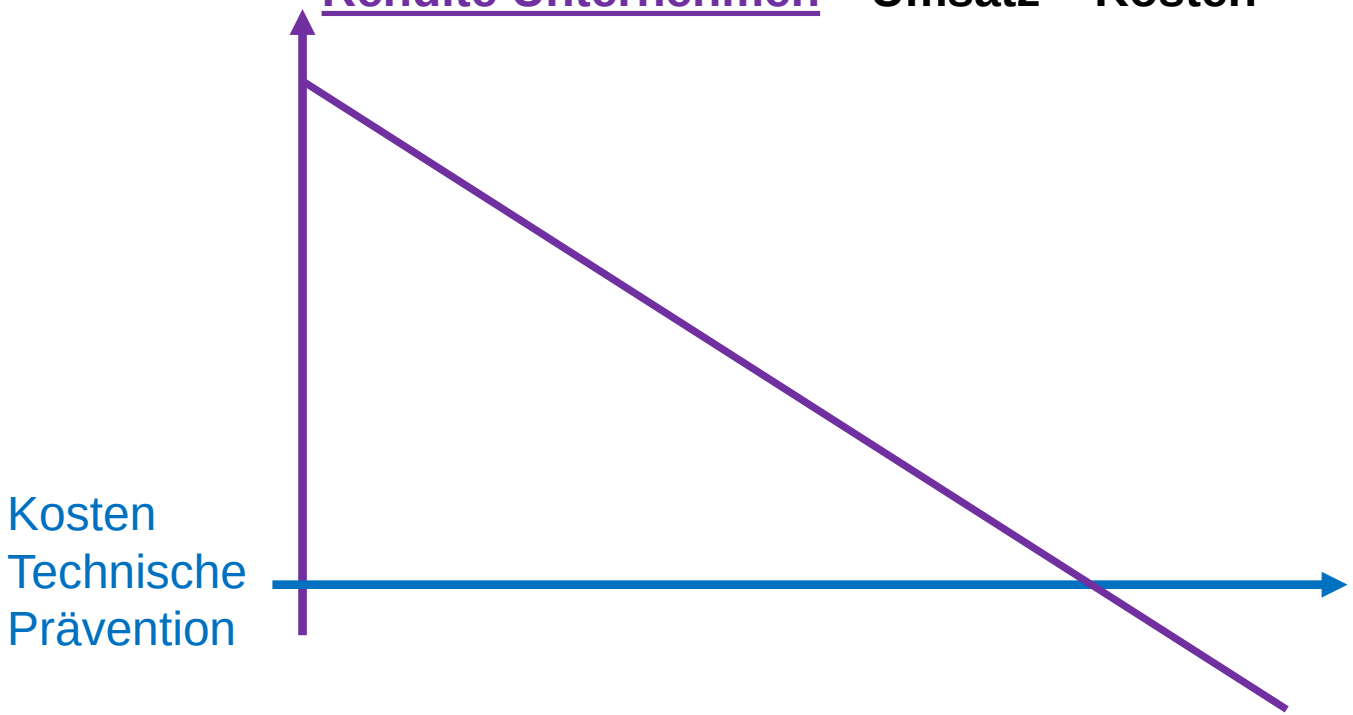


Kosten- / Nutzenrechnung für Cybercrime-Verhaltensprävention

Im nächsten Abschnitt wird das Kosten- / Nutzenverhältnis für die Verhaltensprävention dargelegt.

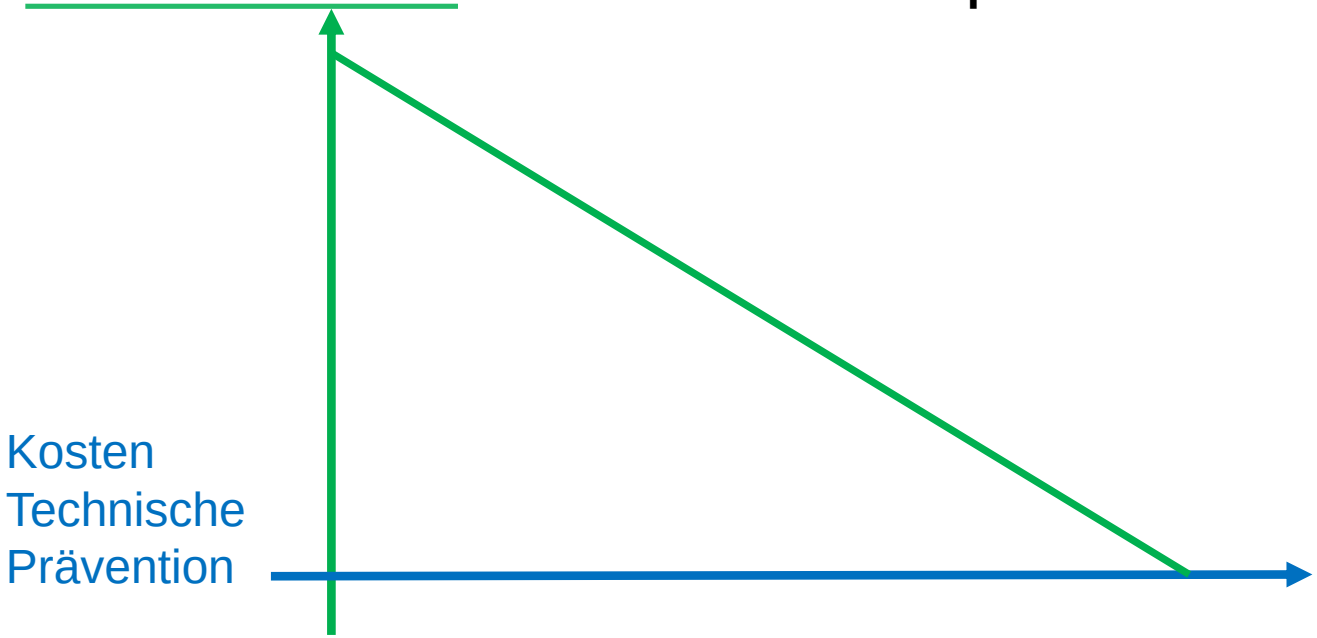
Kosten- / Nutzenrechnung für Cybercrime - Verhaltensprävention

Rendite Unternehmen = Umsatz – Kosten

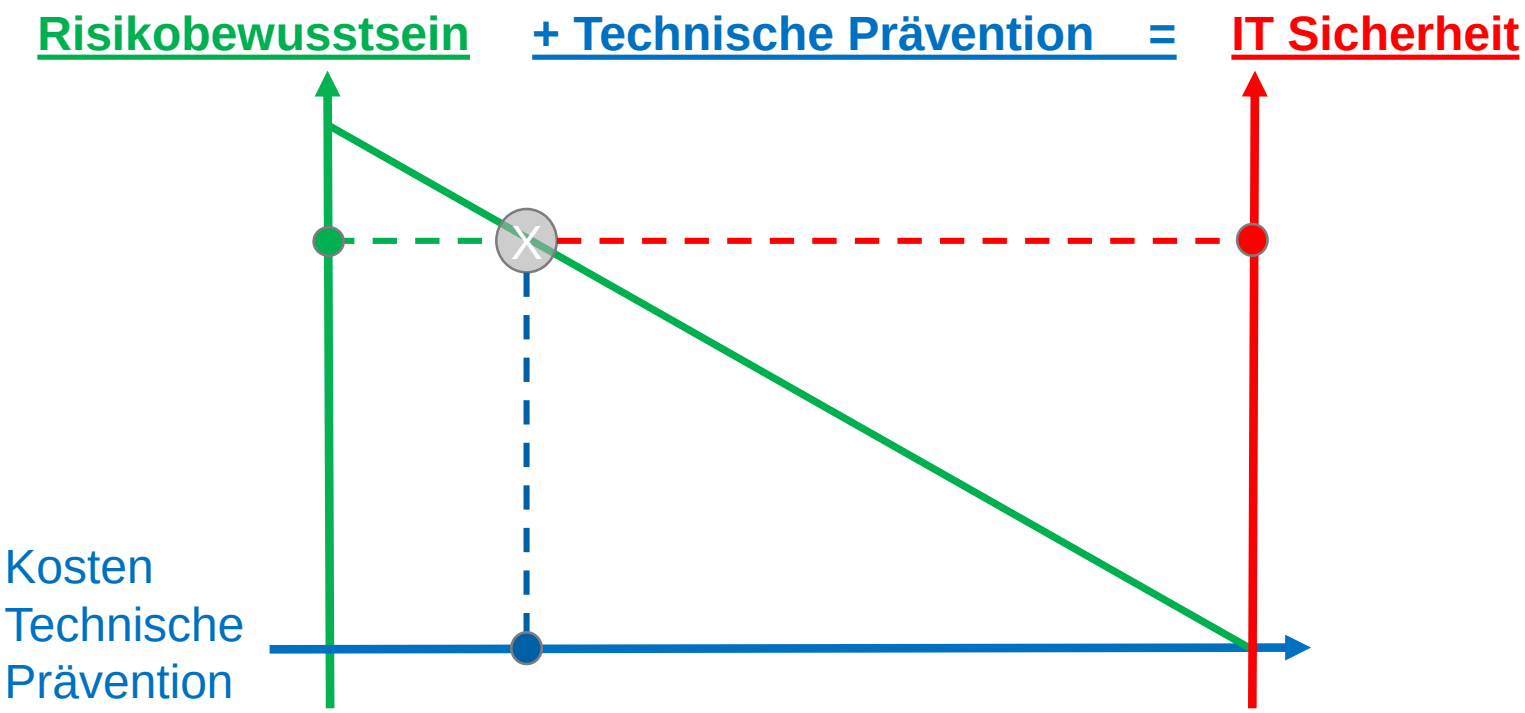


Kosten- / Nutzenrechnung für Cybercrime - Verhaltensprävention

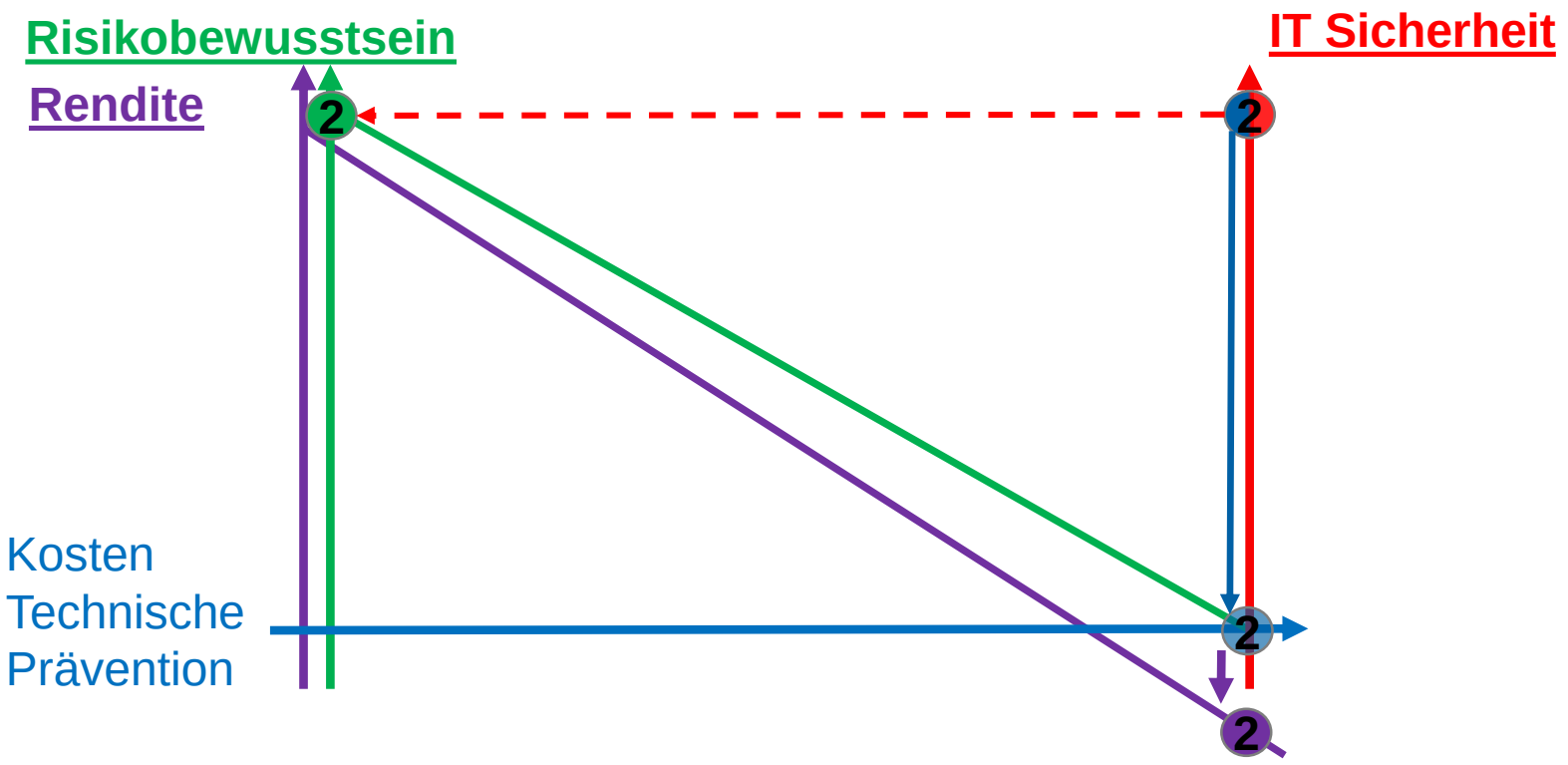
Risikobewusstsein kann Technik z.T. kompensieren



Kosten- / Nutzenrechnung für Cybercrime - Verhaltensprävention

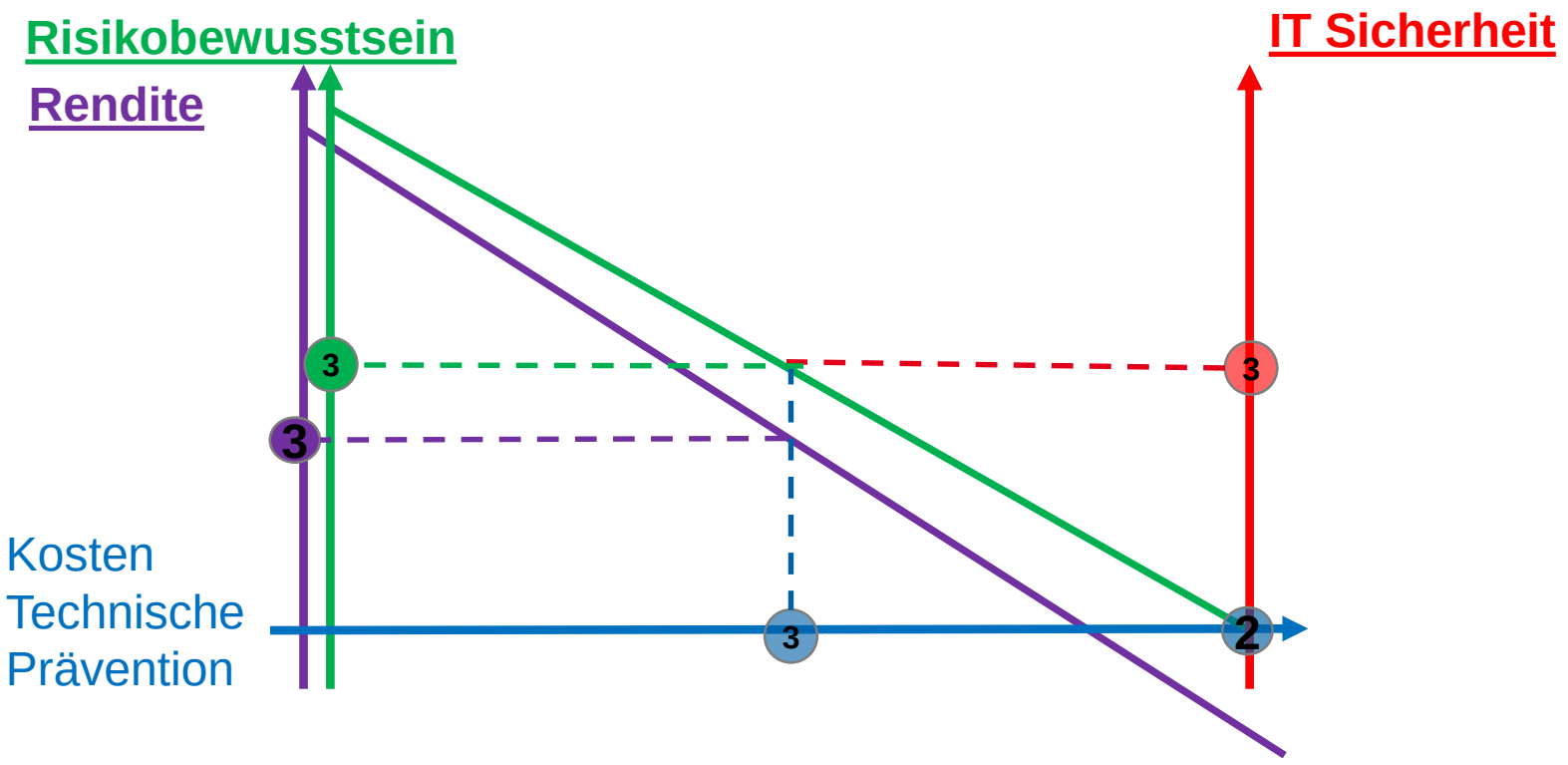


Kosten- / Nutzenrechnung für Cybercrime - Verhaltensprävention



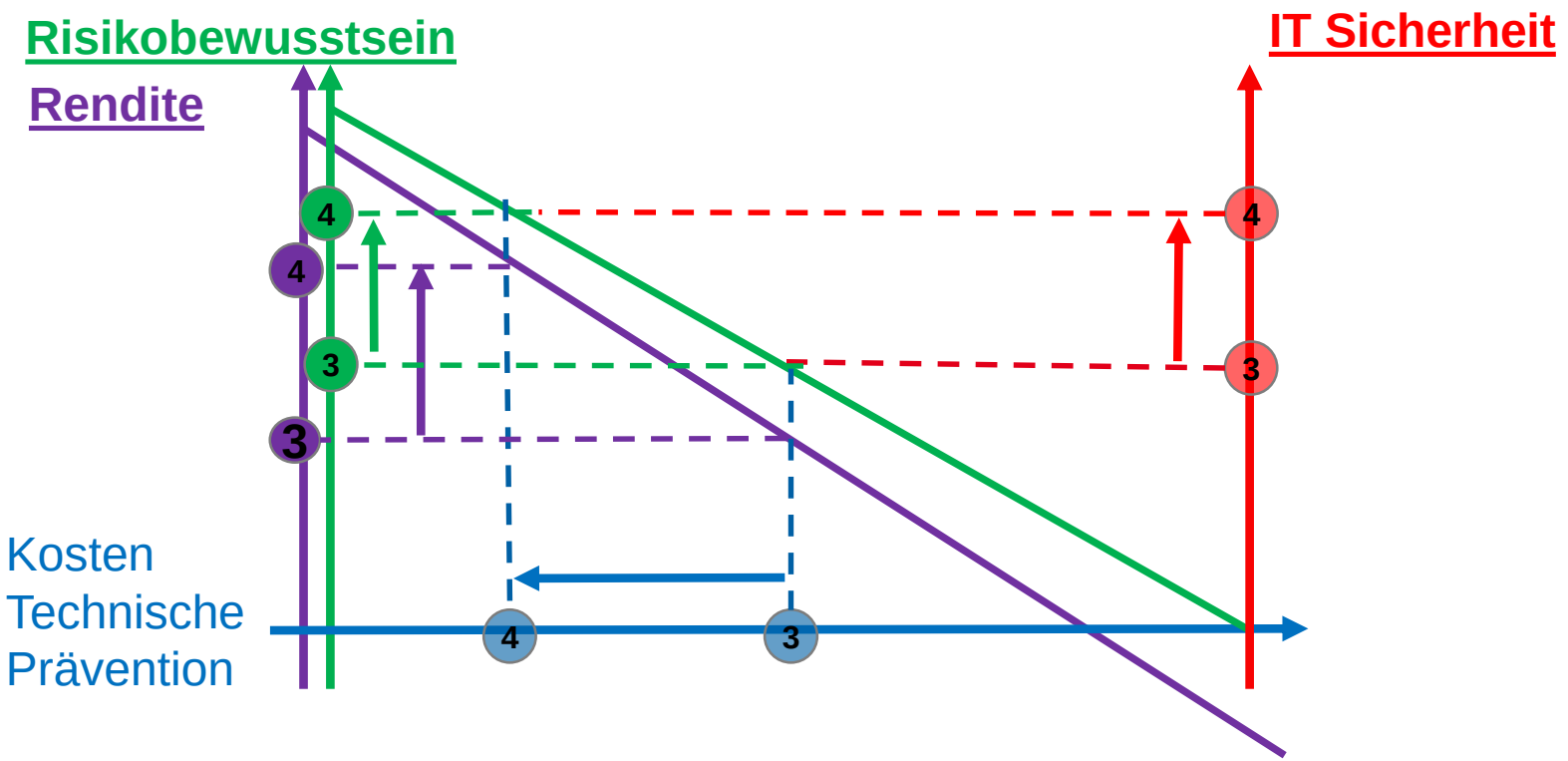
Höchste IT Sicherheit (Risikobewusstsein + Technik) kostet zu viel und schädigt den Gewinn

Kosten- / Nutzenrechnung für Cybercrime - Verhaltensprävention



Mittlere IT Sicherheit (Risikobewusstsein + Technik) ist Durchschnitt und kann den Gewinn gefährden

Kosten- / Nutzenrechnung für Cybercrime - Verhaltensprävention



Ein erhöhtes Risikobewusstsein durch Verhaltensprävention kann technische Fixkosten einsparen und bei gleichzeitiger Erhöhung der IT-Sicherheit auch den Gewinn optimieren.

Vielen Dank für Ihre Aufmerksamkeit.