



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# **Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen**

**- Vorlesung Cyber-Sicherheit -**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

Institut für Internet-Sicherheit – if(is)  
Westfälische Hochschule, Gelsenkirchen  
<http://www.internet-sicherheit.de>

**if(is)**  
internet-sicherheit.

- **Ziele und Ergebnisse der Vorlesung**
- **Einführung**
- **Return on Security Investment (RoSI)**
- **Zusammenfassung**

- **Ziele und Ergebnisse der Vorlesung**
- Einführung
- Return on Security Investment (RoSI)
- Zusammenfassung

# Ziele und Ergebnisse der Vorlesung

## → Wirtschaftlichkeit von Cyber-Sicherheit.

- Gutes Verständnis für die Bewertung der **Wirtschaftlichkeit** von Cyber-Sicherheitsmaßnahmen.
- Erlangen der Kenntnisse über die Berechnung und Bewertung des **Return on Security Investments**.

- Ziele und Ergebnisse der Vorlesung
- **Einführung**
- Return on Security Investment (RoSI)
- Zusammenfassung

- Die Aufgabe von IT-Systemen ist es, die Geschäftsprozesse in Unternehmen zu optimieren und dadurch Kosten zu reduzieren oder den Umsatz zu steigern, um letztlich mehr Profit zu erzielen.
  - Die IT und die IT-Dienstleistungen dienen dem Zweck der Bestandssicherung und Gewinnmaximierung.
- **Minimierungsprinzip:**
  - Ziel ist es, bei einem gesetzten Ziel minimalen Aufwand zu betreiben.
  - Wenn das Ziel ein bestimmter Gewinn ist, müssen bei gleichem Umsatz die Kosten gesenkt werden.
  - Somit soll das Ziel Gewinn (Profit) durch den minimalen Mittelverbrauch (Kosten/Input) erreicht werden.

### ■ Maximierungsprinzip:

- Ziel ist es, mit gegebenen Mitteln ein maximales Ziel zu erreichen.
- Der Gewinn ist dabei eine individuell wählbare Zielvorstellung und soll mit den gegebenen Mitteln maximiert werden.
- Die Mittel (Kosten/Input) sind also vorgegeben, der Umsatz (Output) ist jedoch ein Ziel, das bezüglich des Profits optimiert werden soll.

### ■ Generelles Extremumprinzip:

- Mitteleinsatz und Ergebnis sollen so aufeinander abgestimmt sein, dass der durch sie definierte Prozess, gemessen an problemindividuellen Kriterien, optimal wird.
- Hierbei strebt keine Größe nach einem bestimmten Ergebnis oder Ziel, sondern Kosten und Umsatz stehen in einer variablen Wechselwirkung zu einander.
- Um den Prozess des Wirtschaftens zu optimieren, müssen Arbeitsschritte einer ständigen Qualitätskontrolle unterliegen.
- Diese unterschiedlichen Wirtschaftlichkeitsprinzipien haben nichts mit Cyber-Sicherheit zu tun, sie stellen wirtschaftliche Ziele einer unternehmerischen Tätigkeit da.
- Dabei kann die Bewertung der Wirtschaftlichkeit nach den folgenden Aspekten durchgeführt werden:



### ■ Nach Kostenaspekten:

- Total Cost of Ownership
- Total Cost of Ownership sind die Kosten für Anschaffung, Schulung, Installation, Betrieb, Wartung und Ersatz von IT-Systemen und Cyber-Sicherheitsmaßnahmen.
- Die Berechnung erfolgt durch die Kapitalwert-Methode, d.h. was kostet ein Investment in der Summe aller Aspekte, die berücksichtigt werden müssen?
- Dieser Wert kann mit den Kosten verglichen werden, die z.B. durch einen erfolgten oder geschätzten Schaden und dessen sofortige, mittelfristige und langfristige finanziellen Auswirkungen, entstehen.

- **Nach Nutzenaspekten:**
  - ROI = Return on Investments
  - Hier wird der Nutzen den Kosten gegenübergestellt.
  - Was nützt ein Investment bezüglich Kostenminimierung und/oder Umsatzsteigerung?
  - Wann hat sich eine Investition amortisiert, d.h. die Anschaffungskosten für eine Investition durch den mit der Investition erwirtschafteten Ertrag gedeckt?
  - Je schneller eine Deckung erzielt wird, umso schneller kann ein Gewinn, z.B. durch das Investment von Cyber-Sicherheitsmaßnahmen, generiert werden.

# Einführung

## → Schutzbedarf von IT-Systemen (1/2)

- Der Schutzbedarf wird in IT-Werten bemessen.
- Die Höhe des IT-Wertes zeigt dessen Bedeutung für den Eigentümer und hilft, Cyber-Sicherheitsmaßnahmen ökonomisch und zielgerichtet einzusetzen.
- Zu den IT-Werten gehören u.a. die Daten (Entwicklungsdaten, Vertriebsdaten, Logistikdaten, usw.), IT-Systeme (Hardware) und IT-Anwendungen (Software).
- Um den Schutzbedarf von IT-Werten einheitlich festzustellen, wird ein festgelegter Maßstab benötigt, der bzgl. der Cyber-Sicherheitsbedürfnisse, wie Vertraulichkeit, Authentifikation, Authentizität, Integrität, Verbindlichkeit und Verfügbarkeit festlegt, wann der Schutzbedarf als „niedrig bis mittel“, „hoch“ oder „sehr hoch“ anzusehen ist.

# Einführung

## → Schutzbedarf von IT-Systemen (2/2)

- Wenn dann der Schutzbedarf der IT-Applikationen und Daten gemäß des Schutzbedarfsmaßstabes festgestellt ist, lässt sich der Schutzbedarf für die IT-Systeme einfach ableiten.

- Bei so vielen Risiken und Angriffspotentialen in der IT-Welt, stellt sich unweigerlich die Frage, wie wirksam Cyber-Sicherheitsmaßnahmen überhaupt sein können?
- Wichtiges Kriterium für die Beurteilung ist die Frage:
  - Sind die Cyber-Sicherheitsmaßnahmen auch tatsächlich in der Lage, den realen Angriffen entgegen zu wirken?
- Dabei kann die Stärke der eingesetzten Cyber-Sicherheitsmaßnahmen unterschiedlich bewertet werden.
  - Meist werden hier für die Bewertungen der Wirksamkeit „hoch“, „mittel“ und „niedrig“ verwendet.
- Wichtige Kriterien für die Bewertung der Stärke der Wirksamkeit sind dabei **Fachkenntnisse**, **Ressourcen** und **Gelegenheit** der potentiellen Angreifer.

# Einführung

## → Wie sicher ist „sicher“? (2/5)

- Unter Fachkenntnisse werden alle Kriterien zusammengefasst, die das Anwendungs-Know-how des Angreifers beschreiben.
- Handelt es sich um einen Laien, einen versierten Nutzer (eine kenntnisreiche Person) oder gar einen Experten?
- Ressourcen sind die für einen erfolgreichen Angriff erforderlichen Mittel.
  - Dabei werden die Komponenten Zeit und Ausstattung unterschieden – die Zeit, die zur Durchführung des Angriffs benötigt wird und die erforderliche Ausstattung in Form von Hardware, Werkzeugen und Software.

# Einführung

## → Wie sicher ist „sicher“? (3/5)

- So entstehen Bewertungsbandbreiten von „Sonderausstattung - innerhalb von Monaten“ bis hin zu „Ohne Ausstattung – innerhalb von Minuten“.
- Das Bewertungskriterium „Gelegenheit“ beschreibt im Gegensatz zu den anderen Punkten die eher schwer kontrollierbaren Gegebenheiten wie Zufall, geheime Absprachen und Entdeckung.
- Darunter fällt die eher zufällige Zusammenarbeit mit einem Anwender genauso, wie Absprachen mit dem eigentlich als vertrauenswürdig eingestuften Systemverwalter.
- Daraus ergeben sich Sicherheitsbewertungen, die der jeweiligen Situation entsprechend greifen können.

- So kann eine Cyber-Sicherheitsmaßnahme, die innerhalb von Minuten von einem Laien alleine überwunden werden kann, wohl nicht einmal mehr als „niedrig“ bezüglich der Wirksamkeit eingestuft werden.
- Jedoch könnte eine Cyber-Sicherheitsmaßnahme bezüglich der Wirksamkeit als „hoch“ eingestuft werden, die nur mittels Sonderausstattung und in monatelanger Expertenarbeit in die Knie gezwungen werden kann.
- Ein weiteres Kriterium zur Beurteilung einer Cyber-Sicherheitsmaßnahme ist die Korrektheit.
- Mit dem Faktor Korrektheit soll überprüft und beurteilt werden, ob die Cyber-Sicherheitsmaßnahmen korrekt implementiert sind und wie groß das Vertrauen in die Implementierung der Lösungen ist.



# Einführung

## → Wie sicher ist „sicher“? (5/5)

- Grundsätzlich kann also gesagt werden, dass Cyber-Sicherheitsmaßnahmen nur als wirklich sicher eingestuft werden können, wenn Wirksamkeit, Stärke und Korrektheit zu gleichen Teilen in angemessener Qualität vorherrschen.

# Einführung

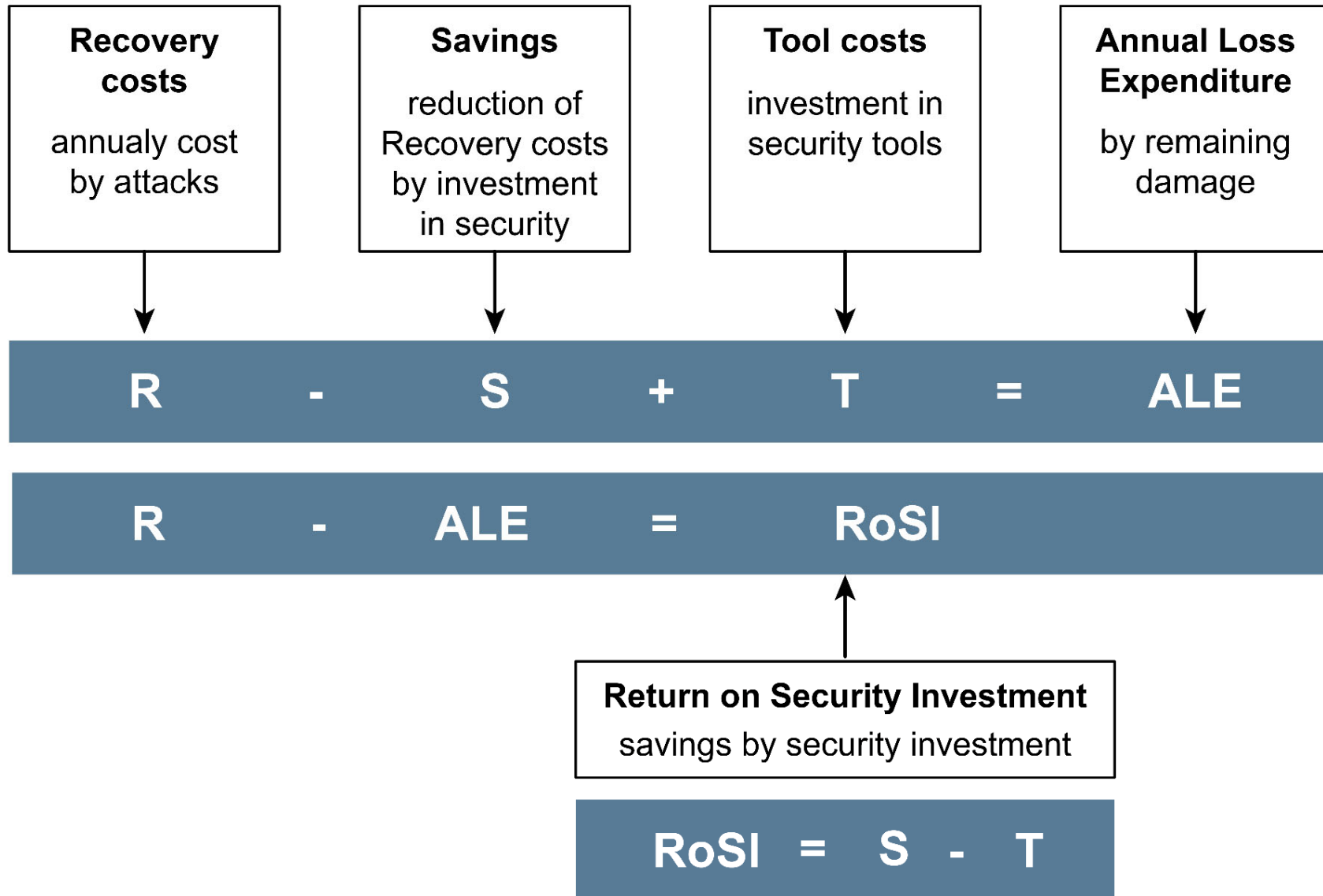
## → Verwundbarkeit

- Die Angriffspotentiale sind für alle Organisationen und Unternehmen gleich.
- Der Unterschied liegt in der Verwundbarkeit, wenn ein Schaden auftritt.
- Durch die oft geringen finanziellen Reserven und Möglichkeiten Geld zu beschaffen, ist die Verwundbarkeit bei klein- und mittelständischen Unternehmen (KMUs) oft ungleich höher als bei sehr großen Unternehmen.
- Die größte Gefahr für den Mittelstand ist das fehlende Bewusstsein für die Notwendigkeit der Cyber-Sicherheit.
- Aber gerade die vielen geschäftsführenden Gesellschafter, deren Existenz unmittelbar mit dem Geschäftserfolg verknüpft ist, sollten hier wachsam sein.

- Ziele und Ergebnisse der Vorlesung
- Einführung
- **Return on Security Investment (RoSI)**
- Zusammenfassung

# Return on Security Investment

## → Nutzenaspekt



# Return on Security Investmen

## → Recovery Costs (1/2)

- Kosten der wahrscheinlichen Schäden.
- Diese Kosten beschreiben alle Aufwendungen, die notwendig sind, um nach einem aufgetretenen Schaden den ursprünglichen Zustand wieder herzustellen.
- Sie werden in die Gesamtkosten der geschäftlichen Tätigkeiten mit einbezogen.
- Die Recovery Costs hängen von dem tatsächlichen Eintritt von Schäden ab, müssen aber aus Erfahrungswerten für die Zukunft abgeschätzt werden.
- In den Recovery Costs können aber auch Aspekte wie die Erhöhung der Fremdkapitalkosten durch z.B. Basel II mit einfließen.

# Return on Security Investmen

## → Recovery Costs (2/2)

- Falls keine geeigneten Cyber-Sicherheitsmaßnahmen eingeführt sind, müssen die Unternehmen für z.B. Investitionskredite mehr Zinsen zahlen.
- Dieses Mehr an Zinsen ist ein Schaden, der auftritt, weil keine angemessene Cyber-Sicherheit im Unternehmen vorhanden ist.
- Durch geeignete Investitionen in Tools kann der Schaden verhindert werden.
- Ein weiterer Aspekt ist die Reduzierung des Prämienaufwands für die Cyber-Versicherung, falls Cyber-Sicherheitsmaßnahmen eingesetzt werden.

# Return on Security Investmen

## → Savings

- Reduzierung der Kosten der wahrscheinlichen Schäden.
- Hierbei handelt es sich um die Kosten, die durch die Einführung von Cyber-Sicherheitsmechanismen (Tools) gespart werden, weil sie mit einer sehr hohen Wahrscheinlichkeit einen Angriff erfolgreich verhindern.
- Auch diese Kosten müssen abgeschätzt werden.

# Return on Security Investmen

## → Tool Costs

- Kosten für Cyber-Sicherheitsmaßnahmen.
- Dies sind die vollständigen Kosten (Total Cost of Ownership - TCO) für die Cyber-Sicherheitsmaßnahmen, die potentielle Angriffe mit einer hohen Wahrscheinlichkeit verhindern sollen.



# Return on Security Investmen

## → Annual Loss Expenditure

- Verbleibende Kosten.
- Das sind die verbleibenen Kosten (Schaden) nach einem Investment in Cyber-Sicherheitsmaßnahmen.

# Return on Security Investmen

## → Return on Security Investment

- gesparte Kosten, erzielter Profit.
- Einsparungen der Recovery Cost (Schäden), die durch das Investment in Cyber-Sicherheitsmaßnahmen erzielt wurden.
- Solange T (Tools), die TCO der Cyber-Sicherheitsmaßnahmen, kleiner sind als S (Savings), die Reduzierung der Kosten, ist RoSI positiv.

$$R - (R - S + T) = \text{RoSI} = S - T$$

# Return on Security Investmen

## → Beispielberechnung RoSI: Notebookverluste (1)

- **Wie hoch ist die Wahrscheinlichkeit des Verlustes eines Notebooks?**
  - Jeder, der die Verantwortung für Notebooks im Unternehmen hat, weiß wie viele Notebooks jährlich aus nachvollziehbaren und nicht nachvollziehbaren Gründen verschwinden.
  - Dennoch ist die offene Kommunikation darüber in den Unternehmen unüblich.
  - Die meisten bekommen ein neues Notebook ohne lange Analysen darüber durchzuführen.
  - Da die meisten sowieso alle 2 bis 3 Jahre ein neues Notebook bekommen, geht die Verlustrate gerade in großen Unternehmen und Organisationen oft in der Masse der neuen Notebooks unter.
  - Im Schnitt werden **6% der Notebooks** jährlich gestohlen oder gehen verloren (Eintrittswahrscheinlichkeit).

# Return on Security Investmen

## → Beispielberechnung RoSI: Notebookverluste (2)

- **Wie hoch ist der Schaden, wenn die Daten, die auf einem Notebook gespeichert sind, von Dritten missbräuchlich verwendet werden?**
  - Schaden kann oft nicht genau analysiert werden (z.B. durch nachträgliche Reduktion des Umsatzes und des Gewinns).
  - Im Schnitt liegt der Schaden pro gestohlenem Notebook bei über 10.000 €.
  - Dies ist nur der Schaden, der durch missbräuchliche Verwendung der Daten entsteht, der Verlust der Hardware, Software und Wiederherstellung eines Ersatzgerätes muss noch zusätzlich betrachtet werden (2.000 € bis 3.000 €).

# Return on Security Investmen

## → Beispielberechnung RoSI: Notebookverluste (3)

- **Cyber-Sicherheitsmaßnahme zum Schutz der Informationen, die auf einem Notebook gespeichert sind.**
  - Um die Kosten abzuschätzen, wird angenommen, dass ein Festplattenverschlüsselungsprodukt verwendet wird.
  - Der Schaden für den Nutzer, für das Unternehmen bleibt bei dem Verlust des Notebooks einschließlich der installierten Software (2.000 bis 3.000 €) und der Wiederbeschaffung und Fertigstellung eines neuen Notebooks begrenzt.
  - Die Anschaffung einer solchen Cyber-Sicherheitsmaßnahme kostet ca. € 110,--, d.h. im Schnitt ca. 4% des Anschaffungspreises eines Notebooks.

# Return on Security Investmen

## → Berechnung der Return on Security Investment (1)

- Beispiel: 500 Mitarbeitern in einem Unternehmen haben ein Notebook mit schützenswerten, wertvollen Daten.
- **Annahmen:**
  - Schaden durch den Verlust der gespeicherten Daten, pro gestohlenem Notebook = € 10.000,--
  - Die Anzahl der Notebooks, die jedes Jahr gestohlen werden, wird mit 6% = 30 Notebooks angenommen.
  - Kosten für das Festplattenverschlüsselungsprodukt: Einmalige Lizenzkosten:  $500 * € 110 = € 55.000$
  - Weitere Kosten (Installation, Roll-Out und Verwaltung): Im ersten Jahr € 10.000,-- und in den folgenden Jahren € 5.000,--.
  - Savings - S:  $30 \text{ Notebooks} * € 10.000 = € 300.000,--$
  - Hier wird nur der Schaden durch die missbräuchliche Verwendung der gespeicherten Daten betrachtet.

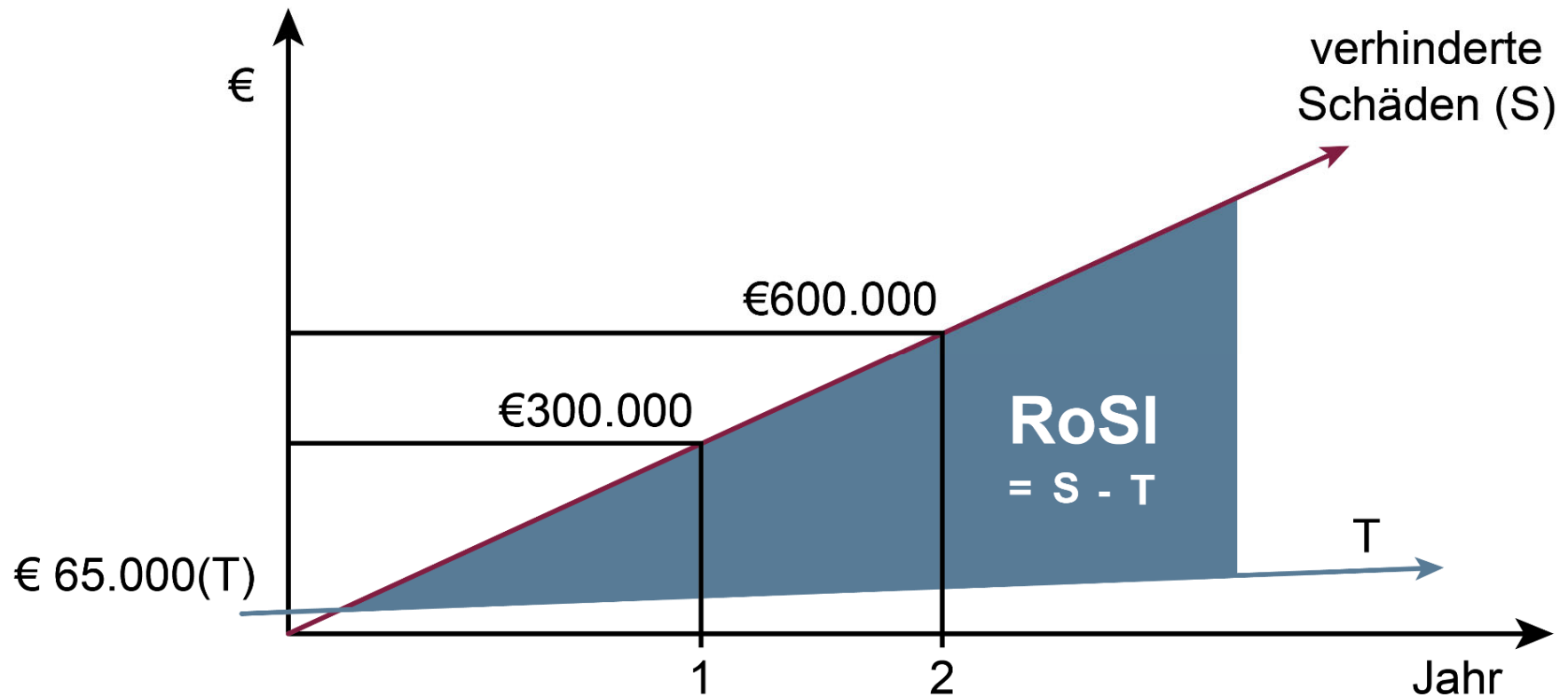
# Return on Security Investment

## → Berechnung der Return on Security Investment (2)

Calculation					In total
Time span	1 <sup>st</sup> year	2 <sup>nd</sup> year	3 <sup>rd</sup> year	4 <sup>th</sup> year	4 years
Initial costs	€55.000	-	-	-	€55.000
Implementation/ Roll-out, Admin	€10.000	€5.000	€5.000	€5.000	€25.000
Reduced costs??	-	-	-	-	-
<b>Value</b> of no losses from sec breaches	€300.000	€300.000	€300.000	€300.000	€1.200.000
ROI 1 <sup>st</sup> year	€235.000				
ROI 2 <sup>nd</sup> year		€530.000			
ROI 3 <sup>rd</sup> year			€825.000		
ROI 4 <sup>th</sup> year				€1.120.000	€1.120.000

# Return on Security Investment

→ Berechnung der Return on Security Investment (3)





# Return on Security Investmen

## → Beispiel mit anderen Annahmen (1)

- Annahmen:
  - Schaden durch den Verlust der gespeicherten Daten, pro gestohlenem Notebook = € 5.000,--
  - Die Anzahl der Notebooks, die jedes Jahr gestohlen werden, wird mit 3% = 15 Notebooks angenommen (Eintrittswahrscheinlichkeit)  
Tool Costs - T (Kosten für das Festplattenverschlüsselungsprodukt)
  - Einmalige Lizenzkosten:  $500 * € 110 = € 55.000$
  - Für die weiteren Kosten von Installation, Roll-Out und Verwaltung wird im ersten Jahr € 10.000,-- und in den folgenden Jahren € 5.000,-- angenommen. Savings - S (vermiedener Schaden)
  - $15 \text{ Notebooks} * € 5.000 = € 75.000,--$

# Return on Security Investmen

## → Beispiel mit anderen Annahmen (2)

Calculation					In total
Time span	1 <sup>st</sup> year	2 <sup>nd</sup> year	3 <sup>rd</sup> year	4 <sup>th</sup> year	4 years
Initial coasts	€55.000	-	-	-	€55.000
Implementation/ Roll-out, Admin	€10.000	€5.000	€5.000	€5.000	€25.000
Reduced costs??	-	-	-	-	-
<b>Value</b> of no losses from sec breaches	€75.000	€75.000	€75.000	€75.000	€300.000
ROI 1 <sup>st</sup> year	€10.000				
ROI 2 <sup>nd</sup> year		€80.000			
ROI 3 <sup>rd</sup> year			€150.000		
ROI 4 <sup>th</sup> year				€220.000	€220.000

# Return on Security Investmen

## → Beispiel mit anderen Annahmen (3)

- Auch bei diesem Beispiel kann aufgezeigt werden, dass schon im ersten Jahr ein ROI von € 10.000,-- erzielt werden kann. Nach vier Jahren liegt der ROI bei € 220.000.
- Weitere Beispiele, bei denen eine RoSI-Berechnung in der Regel einfach durchgeführt werden kann, sind:
  - **Anti-Malware-Lösungen:** Hier haben die meisten Unternehmen in den letzten Jahren selber Zahlen über die Kosten, die durch Schäden bei Malware aufgetreten sind, zur Verfügung.
  - **ID-Management, SingleSignOn (SSO) oder Authentifikation** mit biometrischen Verfahren:
  - Hier kann der Einspareffekt durch Helpdesk-Kosten sehr gut nachgewiesen werden (100 bis 200 €/Jahr pro Nutzer).

# Return on Security Investmen

## → Herausforderungen bei der RoSI-Berechnung

- Die Komplexität bei vielen Berechnungen kommt durch die Abschätzung des direkten und indirekten Schadens eines möglichen erfolgreichen Angriffes und die Beurteilung der Reduzierung des Schadens durch eine spezielle Cyber-Sicherheitsmaßnahme, die dagegen wirkt zustande.
- Weitere, schwer kalkulierbare Aspekte sind zum einem die Beurteilung des direkten Zusammenhangs zwischen einem konkreten Angriff und einem speziellen Schaden und zum anderen die Abschätzung zwischen einem Angriff und der unmittelbaren Wirkung einer Cyber-Sicherheitsmaßnahme.
- Hier müssen in der Praxis die Kosten für die Cyber-Sicherheitsmaßnahmen oft auf verschiedene Schadensfälle, die möglicherweise durch unterschiedliche Angriffe verursacht wurden, anteilig berechnet werden.

- Ziele und Ergebnisse der Vorlesung
- Einführung
- Return on Security Investment (RoSI)
- **Zusammenfassung**

# Wirtschaftlichkeit von Cyber-Sicherheit.

## → Zusammenfassung (1/2)

- Die Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen ist ein zunehmend wichtiger und sehr komplexer Punkt, mit dem sich die Verantwortlichen in Unternehmen, Behörden, aber auch die Regierungen, in einer gesellschaftlichen Verantwortung auseinandersetzen müssen.
- Dennoch gibt es Cyber-Sicherheitsmaßnahmen, die rein wirtschaftlich betrachtet nicht sinnvoll sind und dennoch durchgeführt werden, wie z.B. als gesetzliche Notwendigkeit, wenn es um die Sicherheit von Menschen geht, Militär, Angst oder übertriebenes Sicherheitsgefühl.
- Wenn die Schäden nicht nur zu qualifizieren, sondern auch zu quantifizieren sind, dann kann, wie aufgezeigt wurde, ein Return of Security Investment (RoSI) berechnet und oft auch in der Praxis erzielt.

# Wirtschaftlichkeit von Cyber-Sicherheit.

## → Zusammenfassung (2/2)

- Wenn die Schäden nicht nur zu qualifizieren, sondern auch zu quantifizieren sind, dann kann, wie aufgezeigt wurde, ein Return of Security Investment (RoSI) berechnet und oft auch in der Praxis erzielt.
- Der Einsatz von Cyber-Sicherheitsmaßnahmen kann also weit mehr von Nutzen sein und sollte nicht nur als kostspieliger Nebeneffekt betrachtet werden oder aus Angst vor Haftung oder zur Einhaltung von Gesetzen in Betracht gezogen werden.
- Um diesen Aspekt erfüllen zu können, müssen die Angriffe und die resultierenden Schäden so gut wie möglich dokumentiert werden, damit die tatsächlichen Kosten der Schäden benannt werden können.
- Dazu werden geeignete Hilfsmittel notwendig, die die Kosten von erfolgreichen Angriffen festhalten.



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# Wirtschaftlichkeit von Cyber-Sicherheit

**- Vorlesung Cyber-Sicherheit -**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

Institut für Internet-Sicherheit – if(is)  
Westfälische Hochschule, Gelsenkirchen  
<http://www.internet-sicherheit.de>

**if(is)**  
internet-sicherheit.



## Wir empfehlen

- **Kostenlose App securityNews**



securityNews



- **7. Sinn im Internet (Cyberschutzraum)**

<https://www.youtube.com/cyberschutzraum>



- **Master Internet-Sicherheit**

<https://it-sicherheit.de/master-studieren/>



- **Cyber-Sicherheit**

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2019

- <https://norbert-pohlmann.com/cyber-sicherheit/>



## Quellen Bildmaterial

Eingebettete Piktogramme:

- Institut für Internet-Sicherheit – if(is)

## Besuchen und abonnieren Sie uns :-)

### WWW

<https://www.internet-sicherheit.de>

### Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

### Twitter

[https://twitter.com/ ifis](https://twitter.com/ifis)

### YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

### Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>

## Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.

<https://www.it-sicherheit.de/>

# Literatur

## → Artikel / Bücher

N. Pohlmann: „Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsmechanismen“. In Proceedings der "DACH Security Konferenz 2003 – Bestandsaufnahme und Perspektiven", Hrsg.: Patrick Horster, syssec Verlag, 2003

N. Pohlmann: „Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsmechanismen“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 01/2005

<https://norbert-pohlmann.com/wp-content/uploads/2015/08/155-Wirtschaftlichkeitsbetrachtung-von-IT-Sicherheitsmechanismen-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann: „Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?", Im Journal Kosten & Nutzen von IT-Sicherheit, Hrsg.: M. Mörike, S. Teufel, HMD – Praxis der Wirtschaftsinformatik, dpunkt Verlag, April 2006

<https://norbert-pohlmann.com/wp-content/uploads/2015/08/176-Wie-wirtschaftlich-sind-IT-Sicherheitsmaßnahmen-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019

<https://norbert-pohlmann.com/cyber-sicherheit/>