Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Sichtweisen auf die 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.

Inhalt

- Ziele und Ergebnisse der Vorlesung
- IT-Sicherheitslage
- Cyber-Sicherheitsstrategien
- Cyber-Sicherheitsbedürfnisse
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- Pareto-Prinzip: Cyber-Sicherheit
- Cyber-Sicherheitsschäden
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- IT-Sicherheitslage
- Cyber-Sicherheitsstrategien
- Cyber-Sicherheitsbedürfnisse
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- Pareto-Prinzip: Cyber-Sicherheit
- Cyber-Sicherheitsschäden
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Ziele und Ergebnisse der Vorlesung
→ Grundlagen der IT-Sicherheit

- Gutes Verständnis für einige Aspekte der IT-Sicherheit.
- Erlangen der Kenntnisse über **Idee**, den **Aufbau** und **Konzepte** der IT-Sicherheit.
- Gewinn von praktischen Erfahrungen durch die Darstellung von Beispielen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Ziele und Ergebnisse der Vorlesung
- **IT-Sicherheitslage**
- Cyber-Sicherheitsstrategien
- Cyber-Sicherheitsbedürfnisse
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- Pareto-Prinzip: Cyber-Sicherheit
- Cyber-Sicherheitsschäden
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

IT-Sicherheitslage
→ Einschätzung (1/2)

- Positiv lässt sich resümieren, dass sich die gewünschte **digitale Transformation auf allen Ebenen beschleunigt** und dass der **Wertschöpfungsanteil der IT in allen Produkten** bereits einen hohen Stand erreicht hat zunehmend wächst.
- Aber wir stellen auch fest, dass - seit Beginn der IT - auch mit der Digitalisierung die **IT-Sicherheitsprobleme jedes Jahr größer** werden, also definitiv nicht abnehmen.
- Das bedeutet auch, dass unsere **heutige IT nicht sicher genug** konzipiert und aufgebaut ist, um den **Angriffen intelligenter Hacker** erfolgreich entgegenzuwirken.

- **Grundsätzlichen Herausforderungen**
  - IT-Systeme und -Infrastrukturen werden **immer komplexer** (Steigerung der Abhängigkeiten … Supply-Chain … FB …)
  - Die **Methoden der Angreifer werden ausgefeilter** (Ökosysteme)
  - **Angriffsziele** werden **kontinuierlich lukrativer** (Digitalisierung)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

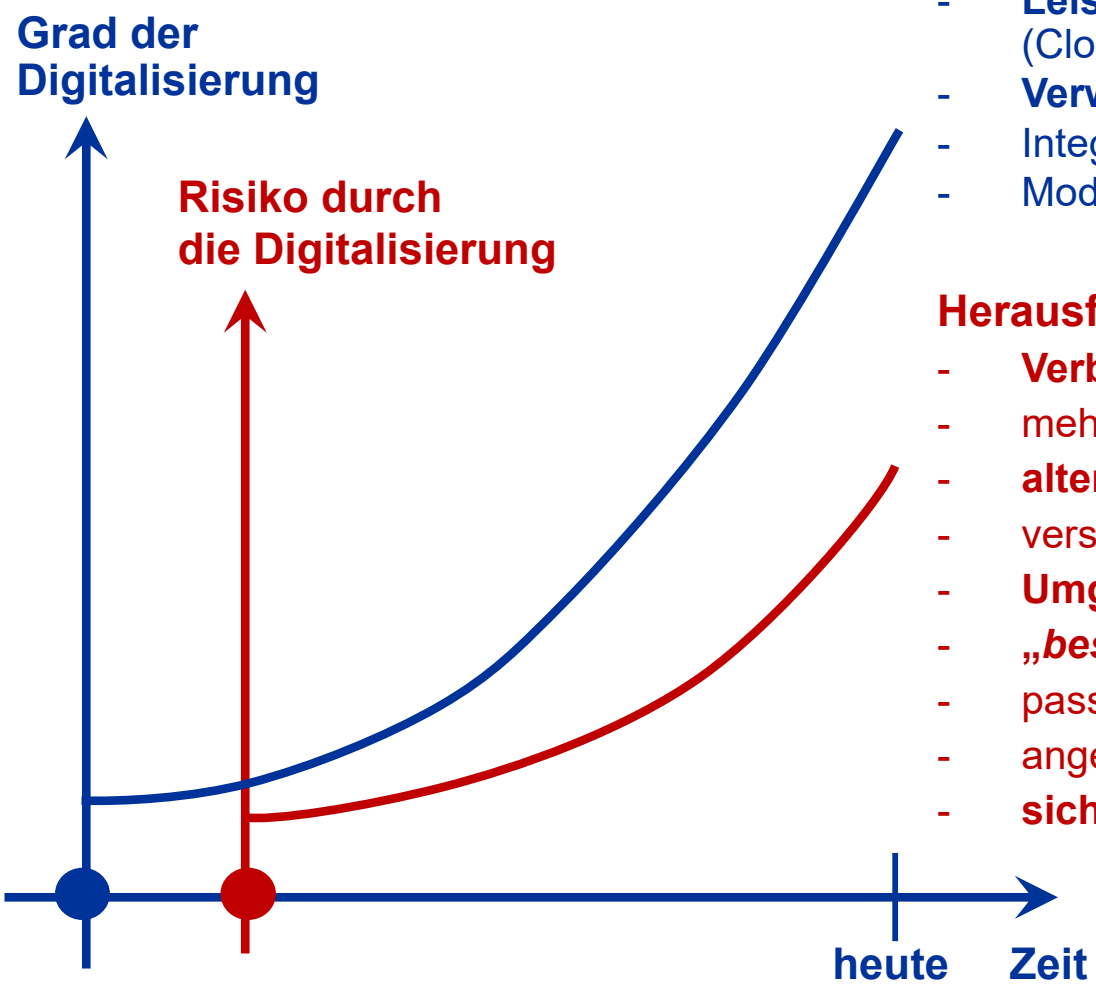
IT-Sicherheitslage
→ Einschätzung (2/2)

- Entsprechend steigen die Risiken sehr stark an, was zu hohen Schäden führt, wie wir auch den aktuellen Umfragen entnehmen können:
- Durch Diebstahl, Spionage und Sabotage entsteht der **deutschen Wirtschaft** jährlich ein **Gesamtschaden von mehr als 220 Milliarden Euro**.

- **Das bedeutet:**
  Die **aktuelle IT-Sicherheitslage** in Deutschland ist **ungenügend** und ist **keine gute Basis** für unsere digitale Zukunft.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Entwicklung der Digitalisierung
→ korrespondierende Risiken



Erfolgsfaktoren der **Digitalisierung** (Beispiele)

- **Kommunikationsinfrastruktur** (5G, Glasfaser, NB, CUG …)
- Smartheit der Endgeräte (Watch, Phone, Book/Pad, IoT …)
- **Leistungsfähigkeit zentraler IT-Systeme** (Cloud, Edge-Computing, Hyperscaler ...)
- **Verwendung von KI** (ML …)
- Integration in IT-Prozesse und IT-Systeme (echtzeitorientiert+)
- Moderne Benutzerschnittstellen (Sprache, Gestik …)

Herausforderungen Cyber-Sicherheit (Beispiele)

- **Verbesserung der Softwarequalität**
- mehr Schutz vor Malware, sichere Webseiten, …
- **alternativen zu Passwörtern (MFA)**,
- verschlüsselte E-Mails, Kommunikation (IPSec, TLS …)
- **Umgang mit der Komplexität der IT-Systeme**, …
- **„*bessere*“ IT-Sicherheitsarchitekturen**
- passenden Level IT-Sicherheit (z.Z. nicht „Stand der Technik“)
- angemessene Verfügbarkeit
- **sichere Hardware** (Sicherheitsmodule in den Komponenten)

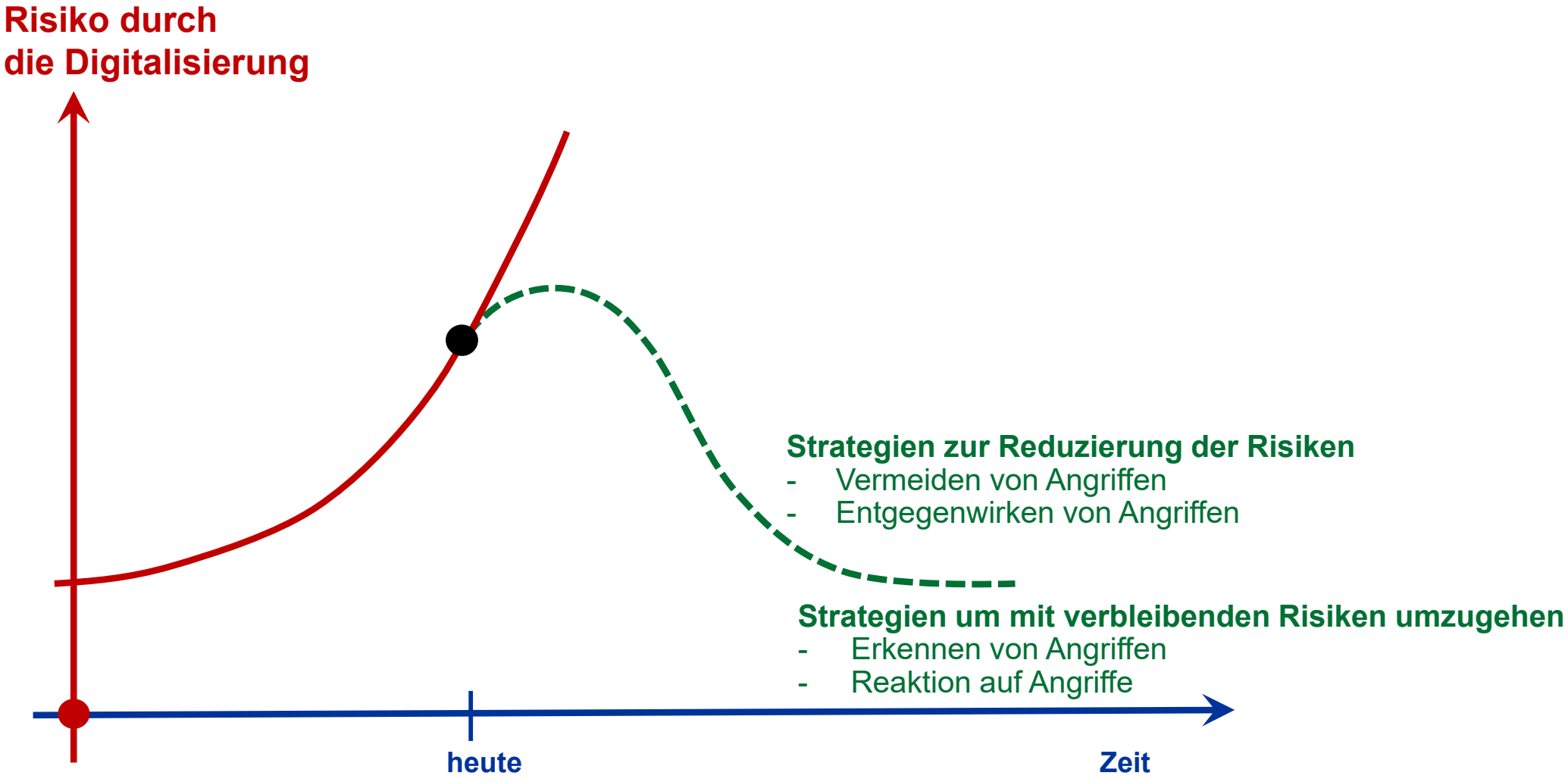
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Ziele und Ergebnisse der Vorlesung
- IT-Sicherheitslage
- **Cyber-Sicherheitsstrategien**
- Cyber-Sicherheitsbedürfnisse
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- Pareto-Prinzip: Cyber-Sicherheit
- Cyber-Sicherheitsschäden
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsstrategien
→ Übersicht



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Vermeiden von Angriffen – (1/4)

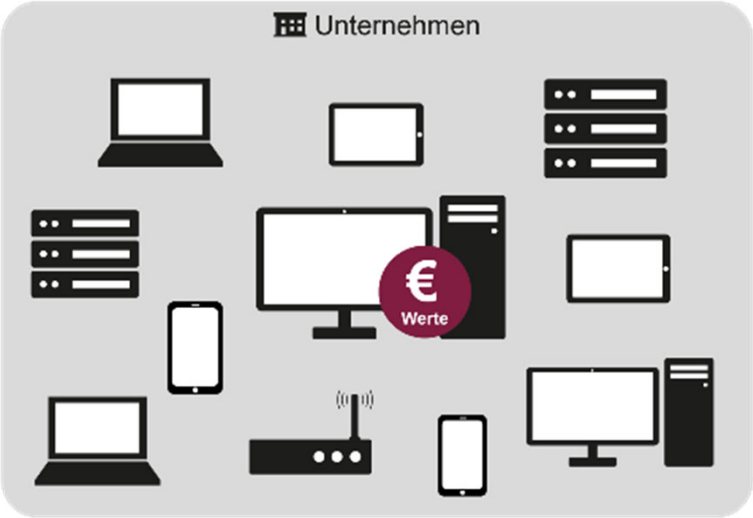
- Eine generelle Cyber-Sicherheitsstrategie zum Schutz der Werte eines Unternehmens ist die Idee einen Schaden durch Angriffe zu vermeiden - **Vermeidungsstrategie**.
- Durch diese Vorgehensweise wird eine Reduzierung der Angriffsfläche und damit die Reduzierung der Risiken erreicht.

- **Prinzip: Digitale Datensparsamkeit**
  - So wenig Daten generieren wie möglich, so viele wie nötig.
- **Prinzip: Nur sichere IT-Technologien, -Produkte und -Dienste verwenden**
  - Keine Technologien, Produkte und Dienste mit bekannten Schwachstellen verwenden (z.B. Browser)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Vermeiden von Angriffen – (2/4)

- **Prinzip: Fokussierung**
  - Im Schnitt sind nur ca. **5 %** aller **vorhandenen Daten** in Unternehmen **besonders schützenswert.**
  - Aber **welche Daten** sind besonders schützenswert und wie können diese angemessen geschützt werden?
  - Aus diesem Grund ist eine **Schutzbedarfsanalyse** notwendig, um diese unternehmenskritischen Daten auf den vorhandenen IT-Systemen zu identifizieren und deren **Schutzbedürfnisse** genau zu kennen.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Vermeiden von Angriffen – (3/4)

- **Prinzip: Reduzierung von IT-Möglichkeiten**
  - Nicht notwendige Software vom IT-System entfernen, nicht verwendete Funktionen einer Anwendung deaktivieren, Kommunikationsmöglichkeiten mithilfe von Routern und Firewall-Systemen reduzieren.

- **Prinzip: Sicherheitsbewusste Mitarbeiter**
  - Sicherheitsbewusstsein setzt sich aus dem **Wissen** und der **Einstellung** der Mitarbeiter eines Unternehmens zusammen.
  - **Relevante Wissen**: Werte eines Unternehmens, Schutzbedarf dieser Werte sowie die Bedrohungen. Organisatorischen Regelungen und die richtige Nutzung von Cyber-Sicherheitsmaßnahmen kennen.
  - Mit der **Einstellung** ist gemeint, dieses **Wissen** zu **verinnerlichen** und zum Schutz des Unternehmens **aktiv umzusetzen**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Vermeiden von Angriffen – (4/4)

- **Bewertung der Vermeidung**
  - Das Vermeiden von Angriffen ist die beste Cyber-Sicherheitsstrategie, um Schäden zu reduzieren.
  - Leider ist die Vermeidungsstrategie jedoch praktisch nur eingeschränkt umsetzbar, da **immer IT-Systeme und Daten benötigt** werden, um die gewünschten digitalen Aktivitäten umzusetzen.
  - Daher reduziert das Vermeiden von Angriffen zwar die Angriffsfläche, aber für die **gewollten IT-Anwendungen und -Dienste** sowie die gewünschten Kommunikationspartner muss eine weitere Cyber-Sicherheitsstrategie, wie das Entgegenwirken von Angriffen eingesetzt werden, um die vorhandenen Risiken weiter zu reduzieren.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Entgegenwirken von Angriffen – (1/4)

- Das Entgegenwirken von Angriffen ist die meistverwendete Cyber-Sicherheitsstrategie, um das vorhandene Risiko zu minimieren und damit Schäden zu vermeiden.
- Dazu werden Cyber-Sicherheitsmechanismen verwendet, die eine **hohe Wirkung** gegen **bekannte Angriffe** zur Verfügung stellen und damit die Werte angemessen schützen.

- Cyber-Sicherheitsmechanismen, die gegen spezielle Angriffe wirken:
  - **Verschlüsselung**
    (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, TLS/SSL ...)
    - Die Verschlüsselung sorgt dafür, dass keine unerlaubten Informationen im Klartext gelesen werden können.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Entgegenwirken von Angriffen – (2/4)

- Cyber-Sicherheitsmechanismen, die gegen spezielle Angriffe wirken:
  - **Multifaktor-Authentifikationsverfahren**
    (Challenge-Response, biometrische Verfahren, …)
    - Mithilfe einer Multifaktor-Authentifikation wird verhindert, dass unerlaubte Nutzer Zugriff auf das IT-System oder den IT-Dienst erhalten.
  - **Anti-Malware-Lösungen**
    (Signatur- oder anomaliebasierte Erkennung)
    - Anti-Malware-Lösungen sorgen dafür, dass illegales Aufspielen und kriminelles Nutzen von Malware nicht umgesetzt werden kann.
  - **Anti-DDoS-Verfahren**
    (On-Site oder Off-Site)
    - Mithilfe von Anti-DDoS-Verfahren wird die erfolgreiche Umsetzung von DDoS-Angriffen verhindert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Entgegenwirken von Angriffen – (3/4)

- Cyber-Sicherheitsmechanismen, die gegen spezielle Angriffe wirken:
  - **Signaturverfahren**
    (verschiedene Formen)
    - Die Nutzung von Signaturverfahren schaffen die Möglichkeit das Leugnen von digitalen Handlungen zu verhindern.
  - **Hardware-Sicherheitsmodule**
    (Smartcards, TPMs, High-Level Security Modules)
    - Mithilfe von Hardware-Sicherheitsmodulen wird der unerlaubte Zugriff und die unerlaubte Nutzung von Sicherheitsinformationen unterbunden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle IT Sicherheitsstrategien
→ Entgegenwirken von Angriffen – (4/4)

- **Bewertung des Entgegenwirkens**
  - Die Cyber-Sicherheitsstrategien „Entgegenwirken von Angriffen“ ist eine naheliegende Vorgehensweise, digitale Werte angemessen zu schützen.
  - Cyber-Sicherheitsmechanismen sollten dem **Stand der Technik** genügen, um eine hohe Wirkung zu haben und dadurch einen angemessenen Cyber-Sicherheitslevel zu erzielen.
  - Leider stehen **nicht genug** oder **nicht schnell genug** wirkungsvolle Cyber-Sicherheitstechnologien, -lösungen und -produkte gegen immer intelligentere Angriffe zur Verfügung oder werden nicht angemessen und umfänglich genug eingesetzt.
  - Da es keine 100-prozentige Cyber-Sicherheit gibt und somit immer ein Restrisiko bleibt, muss mit weiteren Cyber-Sicherheitsstrategien gegen die verbleibenden Risiken vorgegangen werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle Sicherheitsstrategien
→ Erkennen von Angriffen – (1/2)

- Wenn Angriffen nicht angemessen/vollständig entgegengewirkt werden oder eine Vermeidung nicht ausreichend die Angriffsfläche reduzieren kann, dann bleibt noch die Strategie, **Angriffe zu erkennen** und zu versuchen, den Schaden so schnell wie möglich zu minimieren.
- In diesem Bereich spielen prinzipiell Cyber-Sicherheit Frühwarn- und Lagebildsysteme eine besondere Rolle, da sie **Lagebilder erstellen** und **Warnungen erzeugen**, wenn die Bedrohungslage besonders groß wird und gerade umgesetzte Angriffe erkannt werden.

- Hier ist die Idee, dass in einem definierten Bereich (IT- und Kommunikationsinfrastruktur, Endgeräte, …) nach Angriffssignaturen oder Anomalien gesucht wird.
- Wird ein Angriff erkannt, werden die Hintergründe analysiert und passende Gegenmaßnahmen eingeleitet.
- Dadurch ist es möglich entsprechend zu reagieren, damit weitere Schaden noch verhindert oder zumindest reduziert werden kann

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle Sicherheitsstrategien
→ Erkennen von Angriffen – (2/2)

- **Bewertung des Erkennens**
  - Die Cyber-Sicherheitsstrategie „Erkennen von Angriffen“ ist sehr hilfreich, hat aber definierte Grenzen, da es keine 100-prozentige Erkennungsrate gibt.
  - Aus diesem Grund wird es in der Zukunft wichtig, auf diesem Gebiet durch mehr und bessere Sensoren und den unternehmensübergreifenden Austausch viele sicherheitsrelevante Informationen verfügbar zu machen und mit modernen KI-Systemen die Erkennungsraten so hoch wie nur möglich zu bekommen.
  - Außerdem ist es wichtig, schnell und angemessen zu reagieren.
  - Daher müssen die Cyber-Sicherheitsstrategien „Erkennen von Angriffen“ und „Reaktion auf Angriffe“ zusammen betrachtet werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle Sicherheitsstrategien
→ Reaktion auf Angriffe – (1/4)

- Wenn Angriffe erkannt werden, sollte so schnell wie möglich mit passenden Aktionen reagiert werden, die den Schaden im optimalen Fall noch verhindern oder zumindest die Höhe reduzieren.

- **Automatisierte Reaktion**
  - Wenn ein Angriff erkannt wird, können zum Beispiel sofort und (halb-)automatisiert Firewall-Regeln oder E-Mail-Server-Regel so reduziert werden, dass nur noch die wichtigen Prozesse für das Unternehmen aufrechterhalten bleiben.
  - Die Angriffsfläche und damit die potenziellen Schäden werden damit so gut wie möglich verringert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle Sicherheitsstrategien
→ Reaktion auf Angriffe – (2/4)

- **Definition von Befugnissen, Informationsflüsse, Entscheidungsprozess und Kommunikationsstrategien**
  - Für das gesamte Abschalten der Internetverbindung oder die Notwendigkeit des Herunterfahrens vieler IT-Systeme, etwa bei großen Ransomware-Angriffen, müssen in der Regel die Verantwortlichkeiten sowie die damit verbundenen Rechte definiert sein.
  - Um schneller handeln zu können, ist es notwendig die nötigen Informationsflüsse und Reaktionsmöglichkeiten klar ausgearbeitet und vereinbart zu haben.
  - Wichtig für ein angegriffenes Unternehmen sind somit ein sehr kurzer Entscheidungsprozess, effiziente Pfade für die Informationsverteilung sowie klar definierte Befugnisse der Akteure, um im Notfall schnell und verantwortungsvoll reagieren zu können.
  - Zudem muss die Kommunikationsstrategie bezüglich Mitarbeitern, Kunden, Regulierungsbehörden und Medien sorgfältig geplant werden, um einen hohen Imageschaden zu vermeiden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle Sicherheitsstrategien
→ Reaktion auf Angriffe – (3/4)

- **Digitalen Forensik**
  - Eine weitere wichtige Reaktion ist die Analyse eines Angriffs im Sinne der digitalen Forensik.
  - Dadurch lässt sich gewährleisten, dass eventuell vorhandene Lücken geschlossen, vorhandene Cyber-Sicherheitsmaßnahmen optimiert oder weitere integriert werden, damit das Unternehmen zukünftig besser geschützt ist.

- **Notfallplanung**
  - Wichtig ist auch, dass es bereits getestete Reaktionskonzepte (Notfallplanungen) gibt, in denen definiert ist, was im Krisenfall die richtige Vorgehensweise ist und welche Personen die Rechte haben, die entsprechenden Reaktionen im Angriffsfall auszulösen.
  - Besonders relevant ist dabei, alle definierten Reaktionen sehr gut gemeinsam zu trainieren, damit in einem Ernstfall die adäquaten Reaktionen schnell und erfolgreich umgesetzt werden können.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzipielle Sicherheitsstrategien
→ Reaktion auf Angriffe – (4/4)

- **Bewertung der Reaktion**
  - Die Cyber-Sicherheitsstrategie „Reagieren auf Angriffe“ hilft Schäden zu vermeiden oder zu minimieren.
  - Es kann jedoch nur reagiert werden, wenn Angriffe erkannt werden.
  - Notwendig ist auch, die Reaktionskonzepte vorher definiert und getestet zu haben, um in einem Ernstfall auch schnell und wirkungsvoll reagieren zu können.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Ziele und Ergebnisse der Vorlesung
- IT-Sicherheitslage
- Cyber-Sicherheitsstrategien
- **Cyber-Sicherheitsbedürfnisse**
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- Pareto-Prinzip: Cyber-Sicherheit
- Cyber-Sicherheitsschäden
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsbedürfnisse
→ Übersicht (1/3)

- Cyber-Sicherheitsbedürfnisse sind **Grundwerte der Cyber-Sicherheit**, die mithilfe von Cyber-Sicherheitsmechanismen befriedigt werden können.
- Cyber-Sicherheitsbedürfnisse werden auch als Cyber-Sicherheitsziele bezeichnet.

Gewährleistung der Vertraulichkeit

- Vertraulichkeit ist wichtig, damit keine unautorisierten Personen oder Organisationen in der Lage sind, übertragene oder gespeicherte Informationen zu lesen.

Gewährleistung der Authentifikation

- Mithilfe des Cyber-Sicherheitsmechanismus Authentifikation wird verifiziert, wer der Partner bei der Kommunikation oder Transaktion ist beziehungsweise welcher Nutzer auf Betriebsmittel und Informationen zugreift.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsbedürfnisse
→ Übersicht (2/3)

Gewährleistung der Authentizität

- Mithilfe des Cyber-Sicherheitsmechanismus Authentizität wird verifiziert, dass Informationen oder Identitäten echt sind.

Gewährleistung der Integrität

- Beim Cyber-Sicherheitsbedürfnis „Gewährleistung der Integrität“ wird überprüft, ob Informationen, die übertragen werden oder gespeichert sind, unverändert, das heißt original sind.

Gewährleistung der Verbindlichkeit

- Das Cyber-Sicherheitsbedürfnis „Gewährleistung der Verbindlichkeit“ sorgt für die Gewissheit, dass die Prozesse und die damit verbundenen Aktionen auch verbindlich sind.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsbedürfnisse
→ Übersicht (3/3)

Gewährleistung der Verfügbarkeit

- Dieses Cyber-Sicherheitsbedürfnis sorgt für die Gewissheit, dass die Informationen und Dienste auch zur Verfügung stehen.

Gewährleistung der Anonymisierung/Pseudonymisierung

- Mit diesem Cyber-Sicherheitsbedürfnis wird gewährleistet, dass eine Person nicht oder nicht unmittelbar identifiziert werden kann..

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Ziele und Ergebnisse der Vorlesung
- IT-Sicherheitslage
- Cyber-Sicherheitsstrategien
- Cyber-Sicherheitsbedürfnisse
- **Angreifer – Motivationen, Kategorien und Angriffsvektoren**
- Pareto-Prinzip: Cyber-Sicherheit
- Cyber-Sicherheitsschäden
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angreifer
→ Motivationen (1/2)

Anerkennung

- Der Angreifer, typischerweise ein „weißer“ Hacker, greift an, weil er durch einen erfolgreichen Angriff Anerkennung für diese Leistung haben möchte. Ein „weißer“ Hacker verwendet sein Wissen prinzipiell innerhalb der gesetzlichen Rahmenbedingungen.

Geld

- Der Angreifer (IT-Spione, Berufskriminelle, Unternehmens-Cracker, …) greift an, weil er damit gut Geld verdienen kann.

Herausforderung

- Der Angreifer greift an, weil der Angriff für ihn eine Herausforderung und der Erfolg eine Befriedigung darstellt.

Neugierde

- Der Angreifer greift an, weil er durch einen erfolgreichen Angriff seine Neugierde befriedigen kann.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angreifer
→ Motivationen (2/2)

Spaß an der Technik

- Der Angreifer greift an, weil er Spaß an der Technik hat und ein erfolgreicher Angriff dies befriedigt.

Strafverfolgung

- Der Angreifer greift an, weil dadurch Strafverfolgung gesetzlich geregelt umgesetzt werden kann.

Zerstörungswut

- Der Angreifer greift an, weil er die IT und die Informationen zerstören will, zum Beispiel weil der Angreifer ein ehemaliger Mitarbeiter ist und aus seiner Sicht unberechtigt entlassen worden ist.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angreifer
→ Kategorien (1/4)

Hacker

- Hacker brechen in IT-Systeme und Netzwerke ein, weil sie darin eine Herausforderung sehen und mit dem Erfolg ihren Status vergrößern wollen.
- Oft handelt es sich um Jugendliche (Skript-Kiddies), die aus Spieltrieb, also ohne böse Absicht, handeln. Sie sind aber unberechenbar und können hohen Schaden verursachen.

IT-Spione

- Bezahlte Spezialisten – teilweise mit einem sehr hohen Budget – versuchen, über gezielte Angriffe an Informationen zu kommen.
- Ihre Ziele sind politisch oder auch wirtschaftlich begründet.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angreifer
→ Kategorien (2/4)

IT-Terroristen

- Terroristen können IT-Systeme und Netzwerke angreifen, um aus politischen Gründen Angst und Chaos zu verursachen oder ihren Willen umzusetzen.
- Sie wollen oft auf Missstände und/oder politische Ziele aufmerksam machen. Aber auch das Erpressen von Maßnahmen gehört zunehmend dazu.

Unternehmens-Cracker

- Dies sind Mitarbeiter, die auf IT-Systeme und Netzwerke von Konkurrenzunternehmen zugreifen, um ihrem Unternehmen finanzielle Vorteile zu verschaffen.
- Dazu spähen sie beispielsweise Entwicklungsunterlagen, Strategiepläne, Vertriebsinformationen, Kundendaten usw. aus.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angreifer
→ Kategorien (3/4)

Professionelle Kriminelle/Berufskriminelle

- Diese Personen wollen sich mit Angriffen persönlich bereichern, beispielsweise durch die nicht bezahlte Nutzung von Dienstleistungen, durch die unberechtigten Abbuchungen von fremden Konten, Erpressungen (Ransomware, DDoS) usw.

Vandalen

- Das sind Personen, die Angriffe durchführen, um Organisationen oder Personen gezielt Schaden zuzufügen.
- Oft ist die Motivation reine Zerstörungswut.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angreifer
→ Kategorien (4/4)

Penetration Tester

- Cyber-Sicherheitsexperten untersuchen IT-Systeme mit den Mitteln und Methoden eines Hackers, eines professionellen Angreifers, um Schwachstellen für Organisationen zu finden, die dann gestopft werden.

Behörden-Mitarbeiter oder Dienstleister für Behörden

- Mitarbeiter oder Dienstleister der Strafverfolgungsbehörden greifen IT-System und Netzwerke an, um Strafverfolgung zu betreiben.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Definition

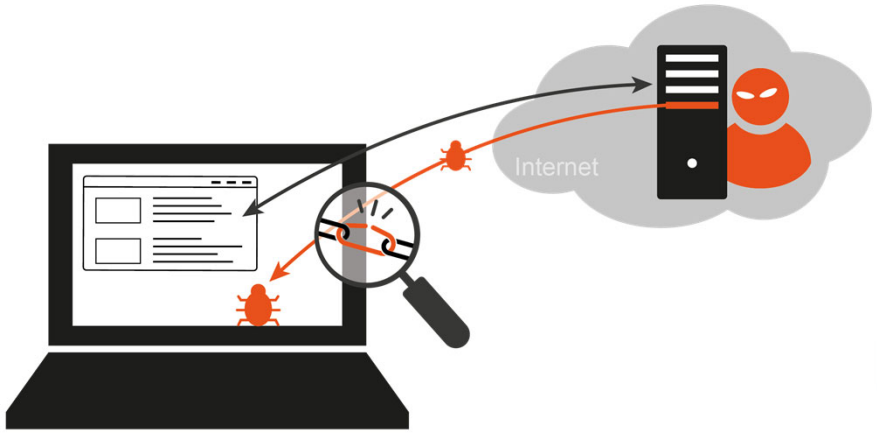
- Ein **Angriffsvektor** bezeichnet sowohl einen **Angriffsweg** als auch eine **Angriffstechnik**, mittels derer ein Angreifer einen **erfolgreichen Angriff** auf ein IT-System oder einen IT-Dienst durchführt.
- Um das Ziel zu erreichen kann dieser Angriffsweg auch verteilt oder mehrstufig sein.
- In der Regel nutzt ein Angreifer dafür **Schwachstellen** in den IT-Systemen, **Social Engineering** bei den Nutzern, **Hacking-Technologien** für die Installation von **Malware** und weitere Angriffstechniken wie **Exploits**, **JavaScript-Code**, Programme zum automatischen Auffinden von Schwachstellen oder **Brute-Force-Angriffe**.
- Um den speziellen Angriff auf dem Opfer-IT-System ausführen zu können, wird die Malware mit Schadfunktion wie zum Beispiel Keylogger, Ransomware, Trojanisches Pferd, Spyware und DDoS-Malware geladen.
- Je mehr potenzielle Angriffsvektoren vorhanden sind, desto höher ist die Wahrscheinlichkeit eines erfolgreichen Angriffs.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (1/12)

Malware-Infiltration über manipulierte Webseiten

- Als erstes wird mit einem gezielten Hacking-Angriff auf den Webserver die Platzierung von Schadsoftware zur Durchführung eines **Drive-by-Downloads** unter Nutzung einer vorhandenen Schwachstelle auf dem Webserver umgesetzt.
- Um einen Nutzer (Opfer) zum Besuch der manipulierten Webseite zu motivieren kann beispielsweise ein Phishing-/Social-Engineering-Angriff durchgeführt werden.
- Beim Zugriff auf die manipulierten Webseiten werden dann beim Drive-by-Download Sicherheitslücken des Browsers oder des Betriebssystems des Opfer-IT-Systems des Nutzers ausgenutzt, um Malware zu installieren.
- Mit der generalisierten installierten Malware kann dann der Angreifer spezielle Schadfunktionen nutzen, um das gekaperte IT-System gemäß seiner Ziele zu manipulieren.

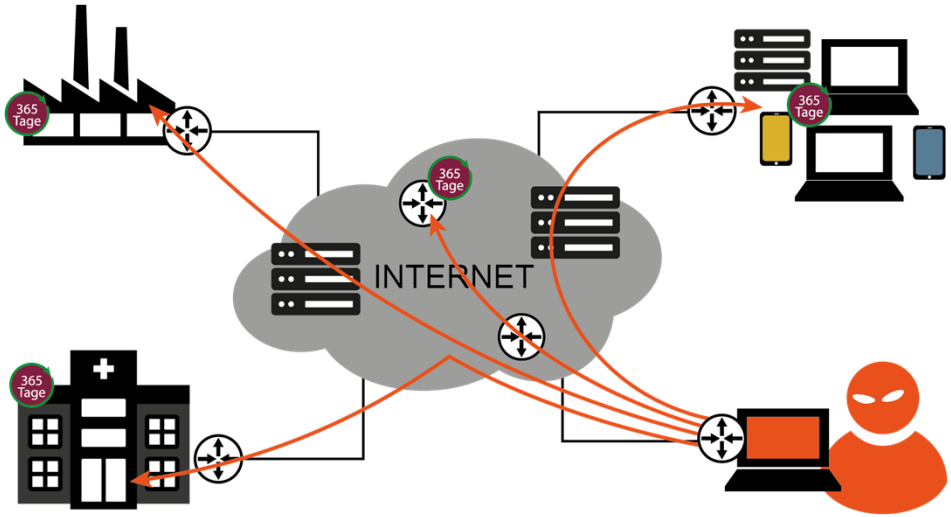


© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (2/12)

Malware-Infiltration über schadhafte E-Mail-Anhänge

- Mithilfe von Sozialen- und Berufsnetzwerken werden die Vorlieben eines potenziellen Opfers analysiert.
- Mit diesen Kenntnissen wird dem Opfer eine persönliche Nachricht gesendet, die perfekt dazu verleitet, auf den Anhang der E-Mail zu klicken.
- Durch das Klicken wird ein Prozess ausgelöst, der ermöglicht, über vorhandene Schwachstellen eine Malware zu installieren.
- Damit ist die Übernahme der Kontrolle über das betroffene Opfer-IT-System umgesetzt.
- Anschließend nutzt der Angreifer entsprechende Schadfunktionen, um seine Ziele auf dem Opfer-IT-System umzusetzen.

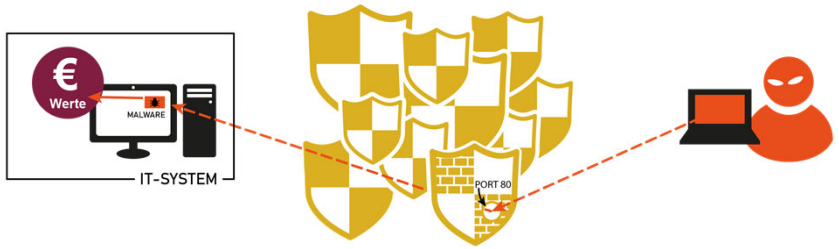


© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (3/12)

Mehrstufiger Angriff auf die IT-Infrastruktur von Unternehmen (APT)

- Ein Angreifer verschafft sich einen ersten Zugang auf ein IT-System in einem Unternehmen, wie in den Beispielen 1 und 2 beschrieben.
- Dann sorgt der Angreifer mit der Schaffung einer individualisierten Malware dafür, dass er den Zugang etabliert, um sich im IT-System frei bewegen zu können und seine Spuren zu verwischen.
- Anschließend verschafft sich der Angreifer mit zusätzlichen Angriffstechniken mehr Administrationsrechte.
- Damit kann er die Kontrolle über weitere IT-Systeme bekommen und lateral in große Teile des Netzwerks zu gelangen.
- So sammelt der Angreifer umfangreiches Wissen über vorhandene Schwachstellen, Funktionen, Werte, usw. auf den IT-Systemen des Unternehmens und kann darüber eine Strategie für den eigentlichen Angriff entwickeln und erfolgreich umsetzen.
- Dieser Vorgehensweise wird auch als Advanced Persistent Threat (APT) bezeichnet.

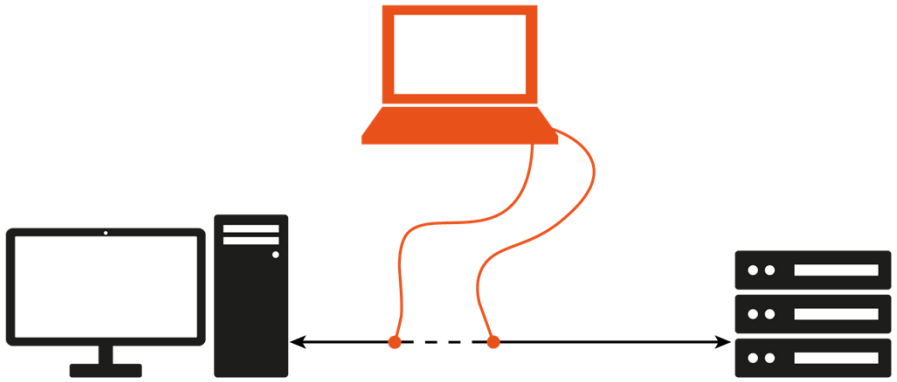


© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (4/12)

Man-in-the-Middle-Angriff (MITM)

- Bei der Man-in-the-Middle-Angriffsmethode schleust sich ein Angreifer aktiv aber heimlich – physisch oder logisch – in die Kommunikation zwischen mindestens zwei Kommunikationspartner, um Daten lesen oder manipulieren zu können.
- Die Kommunikationspartner nehmen dabei an, dass sie direkt und vertraulich miteinander kommunizieren, weil sich der Angreifer jeweils als das wahrgenommene Gegenüber beider Kommunikationspartner ausgibt.
- Durch einen Man-in-the-Middle-Angriff können Passwörter oder weitere wichtige Daten mitgelesen werden, Kommunikationsverbindungen zum Beispiel nach einer Authentifikation übernommen oder Daten manipuliert werden.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (5/12)

Angriff mithilfe eines Software-Updates (Supply Chain-Angriff) – (1/2)

- Bei einem Supply Chain-Angriff oder Lieferketten-Angriff ist die prinzipielle Idee, dass ein vertrauenswürdiger Dienst (Software), der seit längerer Zeit bei einer Organisation/einem Unternehmen in Einsatz ist, irgendwann für einen Angriff verwendet wird.
- Hierfür missbraucht der Angreifer ein legitimiertes Software-Update, das der vertrauenswürdige Softwarehersteller zur Verfügung stellt, um Organisationen/Unternehmen anzugreifen (Angriffsvektor).
- Um diesen Angriff durchführen zu können dringt der Angreifer zuerst in das IT-System des Dienstleisters (Supplier) – dem vertrauenswürdigen Softwarehersteller – ein und infiltriert zum Beispiel das Software-Update mit Malware.
- Voraussetzung für den weiteren Angriff ist, dass dieser Vorgang unbemerkt bleibt, daher muss er an einer bestimmten Prozessstelle umgesetzt werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (6/12)

Angriff mithilfe eines Software-Updates (Supply Chain-Angriff) – (2/2)

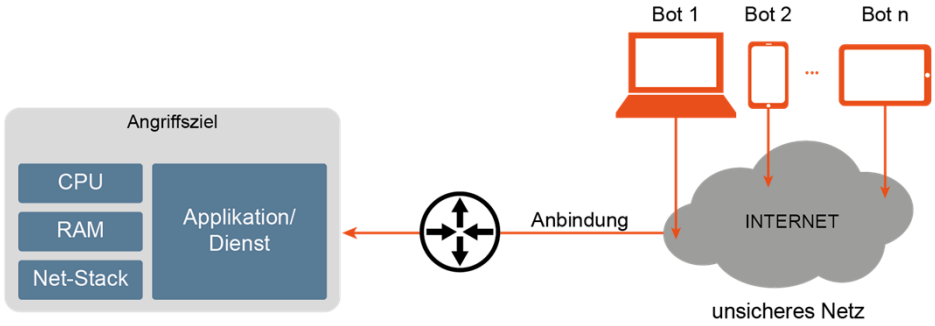
- Nur so lässt sich sicherstellen, dass das manipulierte Software-Update offiziell als Hersteller-Update digital signiert und somit als autorisierter Code vom Kunden akzeptiert und eingespielt wird.
- Darauf basierend kann, in einem zweiten Schritt, der Angreifer bei mehreren Tausend Organisationen gleichzeitig die Software des Herstellers nutzen, um die eigentlichen Angriffe umsetzen.
- Beispiele dieser Angriffsmethode sind: Kaseya und SolarWinds.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (7/12)

Angriff auf die Verfügbarkeit von IT-Systemen (DDoS-Angriff)

- Der Angreifer nutzt die Schwachstelle aus, dass IT-Systeme nur begrenzte Ressourcen (Bandbreite, CPU, RAM …) haben.
- Für den Angriff wird das IT-System gezielt mit einer großen Last spezieller Anfragen überflutet und dadurch überlastet und letztendlich lahmgelegt.
- Dies wird in der Regel unter Einsatz von Botnetzen, bei denen die Bots die Schadfunktion DDoS aktiviert haben, und weiteren Verstärkungsmechanismen wie Reflection und Amplification erfolgreich umgesetzt.



- Die Motivation der Angreifer ist vielfältig:
  - Entweder soll ein IT-System für eine definierte Zeit lahmgelegt werden, um beispielsweise einen Wettbewerber zu behindern oder
  - es steckt eine erpresserische Absicht dahinter, um von dem angegriffenen Unternehmen eine bestimmte Summe verlangen zu können, damit der DDoS-Angriff gestoppt oder gar nicht erst durchgeführt wird.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (8/12)

Missbräuchliche Ausnutzung einer Business-Beziehung mit einem High-Level-Phishing Angriff (1/3)

- Ein Angreifer erlangt mithilfe eines Malware-Keyloggers einen Zugang zu dem E-Mail-Konto von einem Mitarbeiter eines Unternehmens.
- Der Angreifer analysiert kontinuierlich die E-Mails dieses Mitarbeiters dahingehend, wie er diese für einen Angriff verwenden kann.
- Als eine hohe Rechnung an einen langfristigen Kunden über dieses E-Mail-Konto versendet wird, kopiert der Angreifer diese E-Mail zusammen mit allen alten Inhalten. Er verändert in der PDF-Rechnung die Kontonummer und verschickt diese zwei Tage später zusammen mit einer E-Mail, in der er nachfragt, ob die Rechnung bereits beglichen wurde.
- Dies kann er tun, da es sehr unwahrscheinlich ist, dass eine Bezahlung bereits stattgefunden hat.
- Von daher bittet er, dass – falls die Rechnung noch nicht beglichen ist – diese doch an eine neue Kontonummer zu überweisen, da das aufgrund aktueller Sicherheitsgründe notwendig geworden sei.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (9/12)

Missbräuchliche Ausnutzung einer Business-Beziehung mit einem High-Level-Phishing Angriff (2/3)

- Diese E-Mail versendet der Angreifer von einem anderen E-Mail-Konto, damit der Mitarbeiter – dessen E-Mail-Account kompromittiert wurde – den Vorgang nicht mitbekommt.
- Bei dieser E-Mail ist der eigentliche Mitarbeiter als Absender angegeben (Mail-Spoofing). Als Return-Pfad im E-Mail-Header ist jedoch eine andere E-Mail-Adresse angegeben, damit, falls der Empfänger eine Nachfrage hat, diese nicht bei dem Mitarbeiter des Unternehmens ankommt.
- Es ist in diesem Szenario zwingend notwendig, dass der Angreifer diese (eventuelle) E-Mail erhält, damit er entsprechend reagieren kann, ohne dass der Absender davon etwas mitbekommt.
- Für den Empfänger muss es so aussehen, dass die E-Mail von der altbekannten Kundenbeziehung kommt.

- Dies wird dadurch erreicht, dass die Absenderadresse dieselbe ist und Fragmente älterer E-Mail integriert sind.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (10/12)

Missbräuchliche Ausnutzung einer Business-Beziehung mit einem High-Level-Phishing Angriff (3/3)

- Durch diese umfangreiche Vorarbeit ist sichergestellt, dass das angegriffene Unternehmen den geforderten Betrag auf das neue Konto überweist.
- Aufgrund des Zahlungsziels von sechs Wochen fällt es weder dem angegriffenen noch dem kompromittierten Unternehmen früher auf, dass sie einem Phishing-Angriff ausgesetzt waren.
- Daher ist die Verfolgung des Vorfalls sehr schwer bis unmöglich.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (11/12)

Angriff auf einen Steuerberater - eine Geschichte eines erfolgreichen APT-Angriffs (1/2)

- Ein Steuerberater bekommt per E-Mail mitgeteilt, dass ein Angreifer eine Kopie seiner kompletten Mandantenkartei über einen längeren Zeitraum gestohlen hat. Der Steuerberater sollte 100.000 Euro Zahlen, sonst würde der Angreifer den gesamten Datenbestand veröffentlichen.
- Auf die Nachfrage, wie der Steuerberater sichergehen könne, dass er nicht immer wieder zahlen müsse, antwortet der Angreifer, als Zeichen der Vertrauenswürdigkeit, mit einer Referenzliste.
- In dieser Referenzliste standen die Kontaktdaten derjenigen Steuerbüros, die mit einer Zahlung tatsächlich die Veröffentlichung dauerhaft abgewendet haben.
- Eine weitere und spannende Frage war, warum gerade 100.000 Euro, und nicht 50.000 oder 250.000 Euro?

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Angriffsvektoren
→ Beispiele (12/12)

Angriff auf einen Steuerberater - eine Geschichte eines erfolgreichen APT-Angriffs (2/2)

- Dieser Frage sind Experten auf den Grund gegangen, die das Steuerbüro zu Hilfe geholt hat.
- Sie wurden fündig: Der Angreifer hatte sich tief in die IT des Steuerberaters eingenistet.
- Hier waren keine Hobby-Hacker am Werk, sondern ein Profi mit einem langfristigen „Geschäftsmodell“, das die Lösegeldzahlung als einmalige und deshalb für die Opfer lohnenswerte Investition vorsieht.
- Der Angreifer hatten jahrelang jede digitale Bewegung beobachtet, geduldig die betriebswirtschaftliche Entwicklung des Steuerbüros verfolgt, dann plötzlich zugeschlagen.
- Er hatte abgewartet, bis das Geschäft für den Angreifer einträglich, aber zugleich für den Steuerberater wirtschaftlich verkraftbar war.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Ziele und Ergebnisse der Vorlesung
- IT-Sicherheitslage
- Cyber-Sicherheitsstrategien
- Cyber-Sicherheitsbedürfnisse
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- **Pareto-Prinzip: Cyber-Sicherheit**
- Cyber-Sicherheitsschäden
- Zusammenfassung

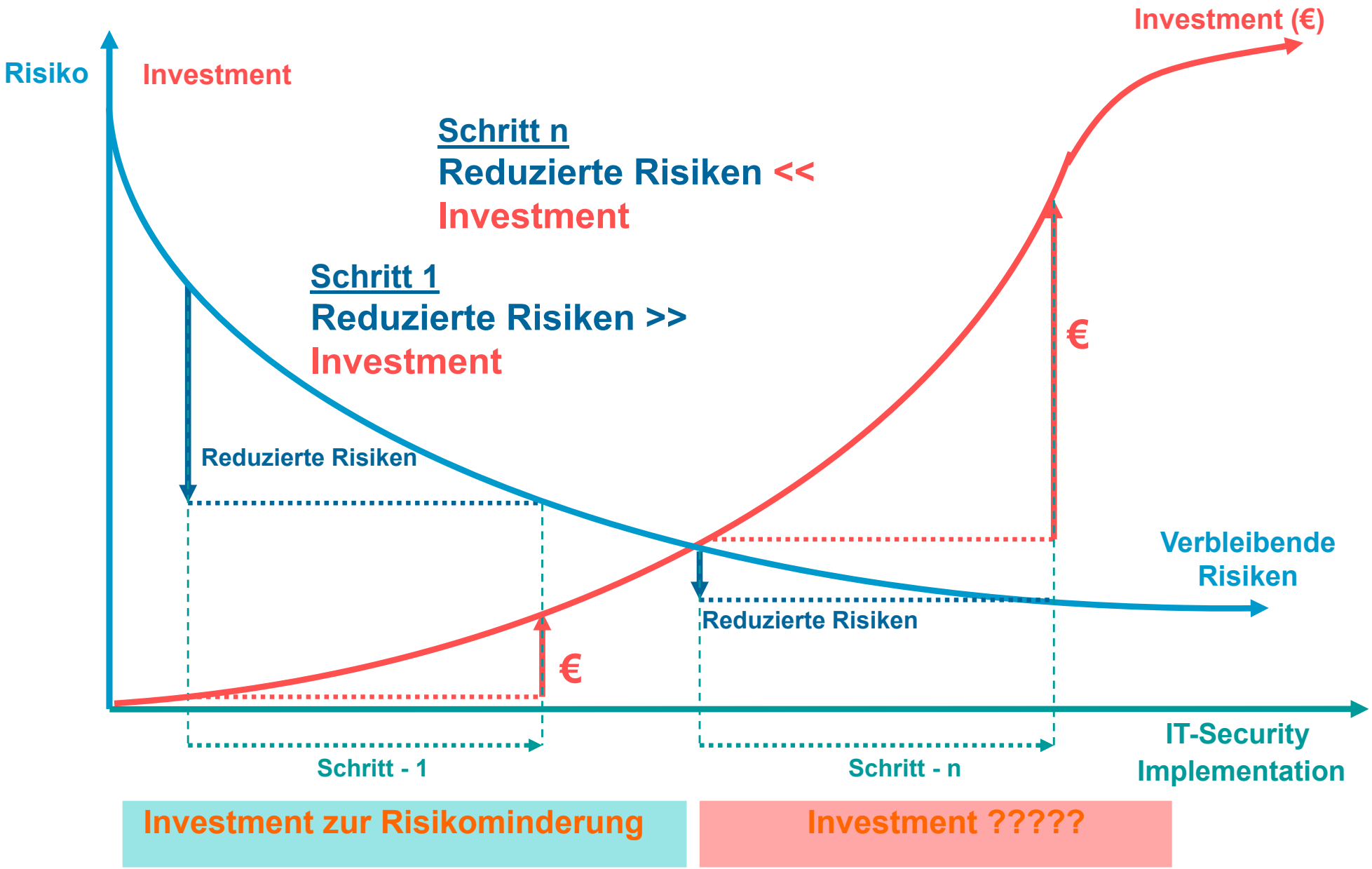
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Pareto-Prinzip
→ Cyber-Sicherheit

- Idee: In einem ersten Schritt wird durch die Implementierung **richtiger Cyber-Sicherheitsmaßnahmen** mit einer **kleinen Investment-Summe** eine **hohe Reduzierung der Risiken** erzielt.
- Dieser Effekt wird auch Pareto-Prinzip oder 80:20-Regel genannt.
- 20 % der richtigen Cyber-Sicherheitsmechanismen richtig eingesetzt liefern 80 % der Reduzierung der Risiken.
- Das bedeutet, dass mit dem Einsatz der richtigen Cyber-Sicherheitsmaßnahmen mit einem relativ geringen Investitionsaufwand ein angemessener Schutz für IT-Systeme hergestellt werden kann.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Pareto-Prinzip
→ Kosten für IT-Sicherheit und Schäden?



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Ziele und Ergebnisse der Vorlesung
- IT-Sicherheitslage
- Cyber-Sicherheitsstrategien
- Cyber-Sicherheitsbedürfnisse
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- Pareto-Prinzip: Cyber-Sicherheit
- **Cyber-Sicherheitsschäden**
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Übersicht

- Ein Cyber-Sicherheitsschaden ist ein materieller oder immaterieller Nachteil, den eine Firma, Organisation oder Person durch ein Ereignis, wie zum Beispiel einen Cyber-Sicherheitsangriff erleidet.
- Der Cyber-Sicherheitsschaden ist immer eine unfreiwillige Einbuße, die der Besitzer an seinen geschützten Rechtsgütern erleidet.

Die Schäden sind im Bereich der Cyber-Sicherheit sehr vielfältig:

- sensible digitale Daten werden auf den IT-Systemen gestohlen
- Informations- u. Produktionssysteme oder Betriebsabläufe werden sabotiert
- digitale Kommunikation wird ausgespäht
- IT- oder Telekommunikationsgeräte werden entwendet
- sensible Daten, die erbeutet werden, sind zum Beispiel:
  - vertrauliche E-Mails
  - Finanzdaten (Umsatz, Gewinn, Kalkulationen …)
  - Personenbezogene und vertrauliche Mitarbeiterdaten (Gehälter, Krankheiten …)
  - Kundendaten (Anfragen, Bestellungen, Preise …)
  - kritische Geschäftsinformationen wie Marktanalysen oder Preisgestaltung
  - …

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Kategorie (1/7)

Verstoß gegen Gesetze/Vorschriften/Verträge

- Verstöße dieser Art können z.B. aus dem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit resultieren.
- Die Schwere des Schadens ist dabei oftmals abhängig davon, ob es sich nur um Bagatellverstöße handelt oder ob daraus rechtliche Konsequenzen für die Institution entstehen können.
- Beispiele für relevante Gesetze:
  Grundgesetz, Bürgerliches Gesetzbuch, Strafgesetzbuch, **Datenschutzgrundverordnung**, **IT-Sicherheitsgesetz**, Sozialgesetzbuch, Handelsgesetzbuch, Personalvertretungsgesetz, Betriebsverfassungsgesetz, Urheberrechtsgesetz, Patentgesetz, Produkthaftungsgesetz.
- Beispiele für relevante Vorschriften:
  - Organisationsanweisungen
  - Dienstvorschriften
- Beispiele für Verträge:
  - Dienstleistungsverträge im Bereich Datenverarbeitung
  - Verträge, die eine Wahrung von Betriebsgeheimnissen vereinbaren

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Kategorien (2/7)

Beeinträchtigung der Aufgabenerfüllung

- Gerade der Verlust der **Verfügbarkeit** eines IT-Systems, eines IT-Dienstes oder der **Integrität der Daten** kann die Aufgabenerfüllung erheblich beeinträchtigen.

- Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen.

- Beispiele:
  - verzögerte Bearbeitung von Verwaltungsvorgängen
  - verspätete Zahlungen aufgrund verzögerter Bearbeitung von Rechnungen
  - das Finden von Material in einem Lager ist nicht möglich, weil die Integrität der Lokalisierungsdaten beschädigt ist
  - Verschlüsselung der Daten auf den Endgeräten durch Ransomware
  - Die Verhinderung der Nutzung von Internet-Diensten durch DDoS-Angriffe

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Kategorien (3/7)

Beeinträchtigung der persönlichen Unversehrtheit

- Fehlfunktion eines IT-Systems oder Anwendung kann:
  - Unmittelbar die Verletzung
  - Die Invalidität
  - Den Tod
- Höhe des Schadens ist direkt an dem persönlichen Schaden zu messen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Kategorien (4/7)

Negative Außenwirkung

- Durch den Verlust eines Grundwerts (Vertraulichkeit, Integrität, Verfügbarkeit) in einem IT-System und IT-Diensten können verschiedenartige negative Außenwirkungen entstehen.
- Beispiele:
  - Renommee- und Vertrauensverlust einer Firma, einer Organisation
  - Beeinträchtigung der Beziehungen zu kooperierenden Behörden oder Unternehmen
  - verlorenes Vertrauen in die Arbeitsqualität
  - Zuspielen vertraulicher Daten an die Presse oder andere Organisationen
- Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlusts und am Verbreitungsgrad der Außenwirkung. Die Ursachen für diese Schäden können vielfältiger Natur sein, zum Beispiel:
  - Handlungsunfähigkeit durch IT-Ausfall
  - fehlerhafte Veröffentlichungen durch manipulierte Daten
  - falsche Berechnungen durch fehlerhafte Kalkulationsprogramme
  - Nichteinhaltung von Schweigepflichten durch Vertraulichkeitsverlust von Daten

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Kategorien (5/7)

Beeinträchtigung des informationellen Selbstbestimmungsrechts

- Verletzung der informationellen Selbstbestimmung
- Missbrauch personenbezogner Daten
- Entsteht bei der Implementierung und dem Betrieb von IT-Systemen und/oder Anwendungen

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Kategorien (6/7)

Fachanwendungsspezifische Schadensszenarien

- Kategorie für „alles andere“
- Hierbei wird betrachtet inwieweit die Vertraulichkeit, Integrität und Verfügbarkeit der Daten unter dem Szenario leiden

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Cyber-Sicherheitsschäden
→ Kategorien (7/7)

Finanzielle Auswirkungen

- Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall eines IT-Systems und -Diensten entstehen.
- Beispiele:
  - unerlaubte Weitergabe von Kalkulationsergebnissen
  - Manipulation finanzwirksamer Daten in einem Abrechnungssystem
  - Einsichtnahme in Strategiepapiere oder Planzahlen
  - Diebstahl von Entwicklungs- und Kundendaten
  - Diebstahl oder Zerstörung von Hardware
- Die Höhe des Gesamtschadens ist bestimmt durch die direkt entstehenden finanziellen Schäden und die daraus resultierenden Folgeschäden.
- Höhe des Schadens grob in 3 Kategorien:
  - ⇒ Bis 25 000 Euro
  - ⇒ 25 000 – 5 Millionen Euro
  - ⇒ Über 5 Millionen Euro

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Ziele und Ergebnisse der Vorlesung
- IT-Sicherheitslage
- Cyber-Sicherheitsstrategien
- Cyber-Sicherheitsbedürfnisse
- Angreifer – Motivationen, Kategorien und Angriffsvektoren
- Pareto-Prinzip: Cyber-Sicherheit
- Cyber-Sicherheitsschäden
- **Zusammenfassung**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Grundlagen der IT-Sicherheit
→ Zusammenfassung (1/2)

- Die aktuelle **IT-Sicherheitslage** in Deutschland ist **ungenügend** und ist **keine gute Basis** für unsere digitale Zukunft.

- Durch die steigende Digitalisierung wird das **Risiko eines Schadens immer größer**, weil damit die **Angriffsziele kontinuierlich lukrativer** werden und die **Angriffsfläche** für die Angreifer **immer größer** wird.

- Um diese Situation im Sinn der Unternehmen zu verbessern werden grundsätzliche Cyber-Sicherheitsstrategien benötigt, die die Cyber-Sicherheitsrisiken strategisch reduzieren.

- **Cyber-Sicherheitsstrategien zur Reduzierung der Risiken:**
  - Vermeiden von Angriffen
  - Entgegenwirken von Angriffen

- **Cyber-Sicherheitsstrategien, um mit verbleibenden Risiken umzugehen**
  - Erkennen von Angriffen
  - Reagieren auf Angriffe

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Grundlagen der IT-Sicherheit
→ Zusammenfassung (2/2)

- Cyber-Sicherheitsbedürfnisse sind **Grundwerte der Cyber-Sicherheit**, die mithilfe von Cyber-Sicherheitsmechanismen befriedigt werden können.

- Neben der Frage der **Motivation**, ist es auch von Bedeutung zu wissen, wer IT-Systeme angreift und welche **Angriffsvektoren** sie nutzen.

- Pareto-Prinzip oder 80:20-Regel:
  20 % der richtigen Cyber-Sicherheitsmechanismen richtig eingesetzt liefern **80 % der Reduzierung der Risiken**.

- Ein **Cyber-Sicherheitsschaden** ist ein materieller oder immaterieller Nachteil, den eine Firma, Organisation oder Person durch ein Ereignis, wie zum Beispiel einen Cyber-Sicherheitsangriff **unfreiwillig erleidet**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Sichtweisen auf die Cyber-Sicherheit

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

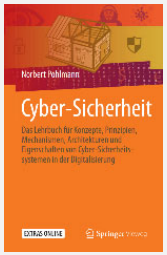
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Anhang / Credits

Wir empfehlen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
  https://norbert-pohlmann.com/cyber-sicherheit/



- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

CYBER SCHUTZRAUM

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

MASTER internet-sicherheit.

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/ProfPohlmann

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

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/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Grundlagen der IT-Sicherheit
→ Bücher, Artikel und Vorträge

Vorlesungen und Übungen aus dem Lehrbuch Cyber-Sicherheit
Unter dem folgenden Links werden 16 Vorlesungen und Übungen aus dem Lehrbuch Cyber-Sicherheit kostenlos zur Verfügung gestellt:

Vorlesungen: https://norbert-pohlmann.com/cyber-sicherheit-vorlesungen/

Übungen: https://norbert-pohlmann.com/cyber-sicherheit/#UebungBuch

Artikel, Vorträge, Bücher, Glossar, …
Auch weitere Bereiche bieten qualitativ hochwertigen Input und vermitteln interessantes Hintergrundwissen.

Artikel: https://norbert-pohlmann.com/category/artikel/

Vorträgen: https://norbert-pohlmann.com/category/vortraege/

Bücher: https://norbert-pohlmann.com/category/buecher/

Glossar: https://norbert-pohlmann.com/glossar-cyber-sicherheit1/

Strategien: https://norbert-pohlmann.com/category/it-strategien/

Statements: https://norbert-pohlmann.com/category/statements/

Studien-Gutachten: https://norbert-pohlmann.com/category/gutachten/

Lehrbuch Cyber-Sicherheit: https://norbert-pohlmann.com/cyber-sicherheit/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen