Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Social Web 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.

Social Web Cyber-Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Soziale Netzwerke
- Fake-News
- Cyber-Mobbing
- Weitere Implikationen
- Zusammenfassung

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

Social Web Cyber-Sicherheit
→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Soziale Netzwerke
- Fake-News
- Cyber-Mobbing
- Weitere Implikationen
- Zusammenfassung

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

Ziele und Ergebnisse der Vorlesung
→ Social Web Cyber-Sicherheit

- Gutes Verständnis für die **Cyber-Sicherheitsprobleme** von Sozialen Netzwerken.
- Erlangen der Kenntnisse über **Fake-News**, **Social Bots, Deep-Fake** und weiteren **Implikationen** von Sozialen Netzwerken.
- Verstehen der **Cyber-Mobbing Problematik** im Cyber-Raum.

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

Social Web Cyber-Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- **Soziale Netzwerke**
- Fake-News
- Cyber-Mobbing
- Weitere Implikationen
- Zusammenfassung

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

Soziale Netzwerke
→ Überblick (1/5)

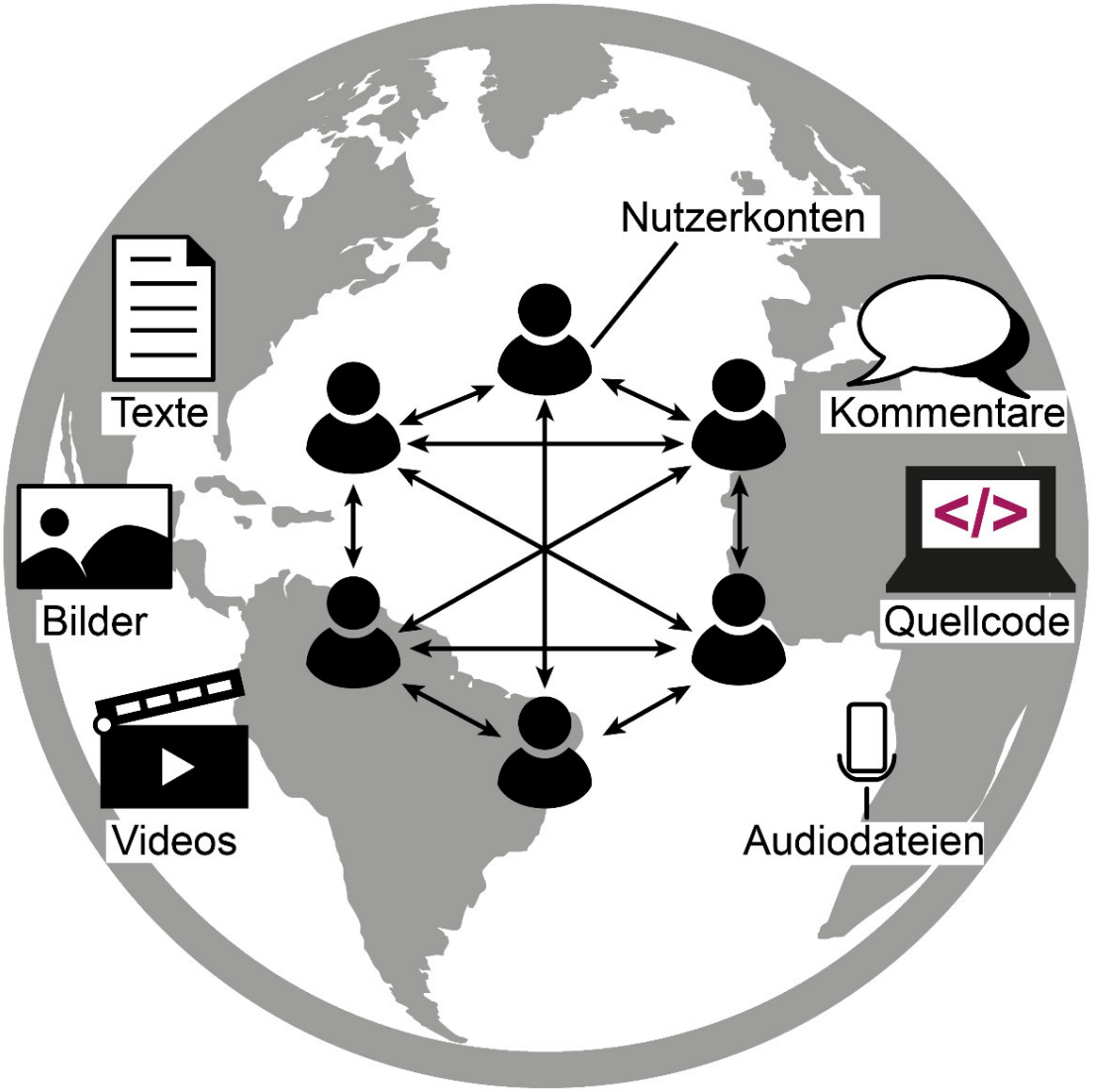
- **Soziale Netzwerke** als **Mitmach-Web** (wie z.B. Facebook, Partnerbörsen, YouTube, XING, Twitter und Co.) bringen Nutzer aus verschiedenen Gesellschaftsgruppen zusammen.

- Soziale Netzwerke schaffen auch neue Wege, Demokratie und Bürgerbeteiligungen zu gestalten.

- Aber der Erfolg der sozialen Netzwerke hat auch bekannte Nachteile und Herausforderungen im Bereich der Cyber-Sicherheit.
  - Social Bots, Fake-News, Deep-Fake und Psychometrie können z.B. auch im Rahmen von Social Engineering Angriffen verwendet werden.

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

Soziale Netzwerke
→ Überblick (2/5)



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

Soziale Netzwerke
→ Überblick (3/5) … 2021

- **Facebook**
  - hat über 2,8 Mrd. Nutzer
  - es werden jeden Tag durch die Nutzer ca. 4 Mrd. Texte, 60 Millionen Bilder und 100 Millionen Stunden Videos eingestellt
- **Instagram**
  - hat über 1 Mrd. Nutzer
  - es werden jeden Tag 95 Millionen Bilder eingestellt und
  - 4,2 Mrd. Likes am Tag durchgeführt
- **Twitter**
  - sind ungefähr 390 Millionen Nutzer registriert und
  - 500 Millionen Tweets am Tag versendet
- **YouTube**
  - hat mehr als 2 Mrd. Nutzer
  - es werden jeden Tag mehr als 100 Millionen Stunden Videos angesehen und
  - ca. 450 Millionen Stunden Videos eingestellt
- **TikTok**
  - hat mehr als 680 Mio. Nutzer,
  - es wurden in einem Jahr täglich mehr als 1 Millionen Videos angesehen.

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

Soziale Netzwerke
→ Überblick (4/5)

- Geschäftsmodel: **„Bezahlen mit persönlichen Daten“** ist für die **informationelle Selbstbestimmung** und den **Datenschutz** ein sehr großes Problem.

- Die große Menge des **„User generated Contents“** wird immer größer und macht zunehmend Probleme.
  - Problematische Inhalte sind z.B. Kinderpornografie, Hate Speech, aber auch Fake News.
  - Es geht aber auch um mit Rechten behaftete Objekte, wie Bilder, Musik, Filme, usw.
  - Inhalte werden anonym veröffentlicht.
  - Betreiber sehen sich „nur als Plattform“.

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

Soziale Netzwerke
→ Überblick (5/5)

- **Social Bots** beeinflussen zielgerichtet Stimmungsbilder und Reputationsverlust z.B. von Politikern und Unternehmen. Beispiele:
  - Ukraine-Konflikt,
  - BREXIT,
  - US-Präsidentschaftswahlkampf,
  - Islamfeindlichkeit,
  - Fremdenhass schüren,
  - Unternehmen diskriminieren und damit Kurse beeinflussen,
  - usw.
- Das Risiko persönlich beleidigt oder diskreditiert zu werden oder Information, die falsch sind, nicht erkennen zu können, wird größer.

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

Soziale Netzwerke
→ Unterschied zu klassischen Medien (1)

- Bei klassischen Medien übernehmen Redakteure die Aufgabe interessante und bedeutsame Beiträge herauszufiltern und für das entsprechende Medium aufzubereiten.
  - Hierbei steht vor allem die Zielgruppe des entsprechenden Mediums im Vordergrund.
  - Ein Redakteur recherchiert auch selbst und schreibt eigene Artikel.
  - Nicht selbst geschriebene Texte werden vom Redakteur redigiert.
  - Aufgabe des Redakteurs ist es die Richtigkeit der Fakten zu überprüfen.
  - Die **Überprüfung der Fakten** ist ein wesentlicher Unterschied zu den Nachrichten, die in sozialen Netzwerken verteilt werden.

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

Soziale Netzwerke
→ Unterschied zu klassischen Medien (2)

- Aus diesem Grund treten Fake-News bei den klassischen Medien relativ selten auf.
  - Wird eine Nachricht im Nachhinein als Fake-News erkannt, wird die Fake-News entfernt und dies in einer **Klarstellung** dokumentiert.

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

Soziale Netzwerke

→ Unterschied Meinungsfreiheit und Fake-News (1)

- **In Artikel 5 des Grundgesetzes steht:**
  - Jeder hat **das Recht**, **seine Meinung** in Wort, Schrift und Bild **frei zu äußern** und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten.
  - Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet.
  - **Eine Zensur findet nicht statt**.
- Die „Meinung“ ist der Ausdruck einer persönlichen Auffassung, die jemand von einer Sache hat.
  - Dies kann uns gefallen oder nicht.
  - **Die Toleranz unterschiedlicher Meinungen ist ein wichtiger Garant für eine funktionierende Demokratie.**

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

Soziale Netzwerke

→ Unterschied Meinungsfreiheit und Fake-News (2)

- Eine **Fake-News ist eine Falschmeldung**, die auf falschen Tatsachen beruht, und damit **unabhängig von** einer bestimmten **Meinung falsch ist**.

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

Social Web Cyber-Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Soziale Netzwerke
- **Fake-News**
- Cyber-Mobbing
- Weitere Implikationen
- Zusammenfassung

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

Fake-News
→ Was ist eine Fake-News?

- Fake-News sind **Falschmeldungen**, die sich insbesondere in sozialen Netzwerken und anderen sozialen Medien verbreiten.

- Fake-News sind **frei erfunden** und sollen die **Konsumenten bewusst täuschen**.

- Im weiteren Sinne werden oft auch solche Nachrichten zu den Fake-News gezählt, die zwar einen wahren Kern besitzen, deren **Aussagen** aber **verfälscht** oder **dekontextualisiert** wurden (zum Beispiel durch irreführende Überschriften).

- Aber auch **satirische Nachrichten** können im weiteren Sinne ebenfalls als eine Art Fake-News bezeichnet werden, falls diese von den Lesern nicht als Satire erkannt werden.

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

Fake-News
→ Beispiel von Fake-News

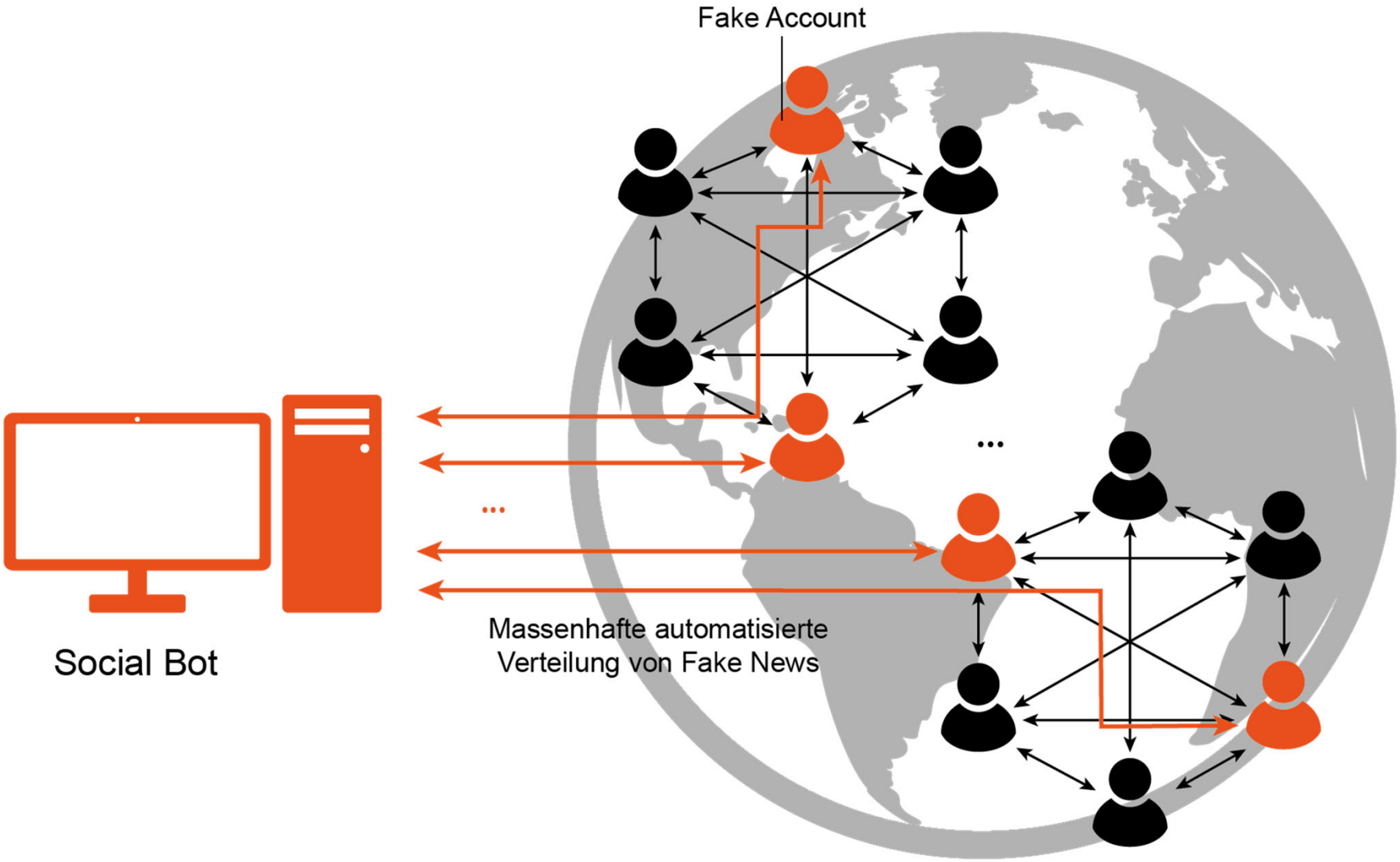
Frei erfundene Nachricht

Aussage verfälscht

Satire

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

Fake-News
→ Social Bot (1/4)



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

Fake-News
→ Social Bot (2/4)

- Damit Fake-News eine sehr große Verbreitung und damit eine starke Wirkung haben, werden sogenannte Social Bots genutzt.
  - Social Bots sind die digitalen Propaganda-Maschinen.
  - Ein Bot ist ein Roboter, ein autonom agierendes Programm im Internet.
  - Eine Social Bot ist ein Meinungsrobotor, der in den sozialen Netzwerken aktiv ist.
  - Social Bots erstellen sehr viele Fake-Accounts und simulieren menschliches Verhalten.
  - Sie werden programmiert und eingesetzt, um gezielt Meinungen im Internet massenhaft automatisiert zu verbreiten.
  - Das Ziel von Social Bots ist es, durch ein verzerrtes Stimmungsbild, eine größere Gruppe oder Gesellschaft in eine bestimmte Richtung zu beeinflussen.

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

Fake-News
→ Social Bot (3/4)

- Zwischen **9 und 15 %** der Twitter-Konten sind nach Schätzungen von US-Forschern nicht menschlich, sondern Bot-gesteuert.

- Aber auch bei Facebook werden sehr viele Accounts von Social Bots betrieben.
  - In der Summe gibt es bei Facebook 6 % Fake-Accounts.
  - Aber nicht alle Fake-Accounts werden von Social Bots verwendet.

- Das Beeinflussungspotential von Social Bots ist sehr groß.
  - Insbesondere wenn bei Entscheidungen nur eine knappe Mehrheit erwartet wird, haben Social Bots einen besonderen Einfluss.

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

Fake-News

→ Wie können Fake-News erkannt werden? (1)

- **Der Nutzer findet selber heraus, ob es sich um eine Fake-News handelt. Empfehlungen von Facebook:**

Lies Überschriften kritisch! → Wenn Behauptungen **unglaublich klingen**, sind sie es vermutlich auch.
Sieh dir die URL genau an! → Unechte oder nachahmende URL → Falschmeldung
Überprüfe die Quelle! → Für ihre Glaubwürdigkeit bekannt?
Achte auf ungewöhnliche Formatierungen! → Tippfehler, seltsame Layouts → Falschmeldung
Sieh dir Fotos genau an! → Manipulierte Bilder, Videos → Falschmeldung
Überprüfe die Datumsangabe! → Geänderte Datumsangabe, chronologisch unlogisch → Falschmeldung
Überprüfe die Beweise! → Mangelnde Beweise, Verweis auf ungenannte Experten → Falschmeldung
Sieh dir andere Berichte an! → Keine anderen Nachrichtenquellen mit derselben Meldung → Falschmeldung
Ist die Meldung ein Scherz? → Wenn Scherz (Humor, Satire, Parodie, …) → *keine* Falschmeldung
Einige Meldungen sind bewusst falsch. → Nur teilen, wenn glaubwürdig

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

Fake-News

→ Wie können Fake-News erkannt werden? (2)

- **Automatische Erkennung:**
  - Grundsätzlich könnten die Vorschläge von Facebook auch durch passende Programme automatisch analysiert werden.
  - Die Ergebnisse werden auf jeden Fall schneller, und es können sehr viele Nachrichten parallel überprüft werden.

- **Erkennen von Fake-News mit Hilfe von KI-Algorithmen:**
  - In den letzten Jahren sind insbesondere im Bereich der Neuronalen Netze (deep neural networks – DNN) enorme Fortschritte erzielt worden.
  - Ein NN ist ein komplexes mathematisches System, das Aufgaben erlernt, indem es gewaltige Datenmengen analysiert.
  - In diesem Bereich werden die größten Erfolge in der Zukunft erwartet.

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

Fake-News

→ Wie können Fake-News erkannt werden? (3)

- **Journalisten werde mit der Prüfung beauftragt:**
  - Journalisten lernen und setzen das Redigieren bereits für die klassischen Medien erfolgreich um.
  - Das Problem dabei ist, dass eine sehr große Anzahl von Journalisten notwendig ist, um diese Aufgabenstellung z.B. für Facebook erfüllen zu können.
  - Wahrscheinlich müssten es mindestens 10.000 Journalisten sein.

- **Was ist zu tun, wenn ich weiß, dass es sich um eine Fake-News handelt?**
  - Wenn ein Betreiber eines sozialen Netzes weiß, dass eine Nachricht eine Fake-News ist, kann er diese mit einen Warnhinweis behaften, oder er kann sie löschen.

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

Fake-News

→ Wie können Fake-News erkannt werden? (4)

- **Warnhinweis:**
  - Da es immer eine Wahrscheinlichkeit gibt, dass eine erkannte Fake-News doch wahr ist, wäre die Kennzeichnung daher im Sinne der Meinungsfreiheit eine gute Kompromisslösung.
  - Der große Nachteil ist, dass Nutzer, die aufgrund ihres Weltbildes oder Voreinstellung diese Falschinformation eher glauben, mit einer hoher Wahrscheinlichkeit nach einer Zeit sich noch an die inhaltlichen Information erinnern werden, nicht aber an den Fake-News-Warnhinweis (Speeper Effect).

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

Fake-News

→ Wie können Fake-News erkannt werden? (5)

- **Löschen von Fake-News:**
  - Im von der Bundesregierung eingebrachten Netzwerkdurchsetzungsgesetz ist das zügige Löschen von Fake-News durch die Betreiber von sozialen Netzwertwerken-Plattformen vorgesehen.
  - Eine der größten Nachteile dieser Methode ist, dass die Betreiber von sozialen Netzwertwerken-Plattformen Inhalte vorsorglich löschen, wenn nur ein Verdacht besteht, es könne sich um strafrechtlich relevante Unwahrheiten handeln.
  - Die Androhung von Strafzahlungen ist so hoch, dass dieses Verhalten sehr wahrscheinlich eintreten wird.
  - Das bedeutet aber, dass viele Nachrichten gelöscht werden, die keine Fake-News sind.
  - Das wiederrum berührt das Recht auf Meinungsfreiheit.

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

Fake-News

→ Wann soll eine Nachricht überprüft werden? (1)

- **Immer dann, wenn ein Inhalt eingestellt wird.**
  - Problem: Bei Facebook müssten am Tag 4 Mrd. Texte, 60 Millionen Bilder und sehr viel Videos überprüft werden.
  - Bei Twitter müssten am Tag 500 Millionen Tweets überprüft werden, bevor sie versendet werden können.
  - 10.000 Journalisten bei Facebook → 400.000 Texte pro Tag.
  - 20 Texte pro Tag → 200.000.000 Journalisten.
  - Praktisch nicht realisierbar.
  - Es wird ein sehr guter Algorithmus benötigt.
  - Nur für die schwierigen Fälle könnte ein Journalist eingebunden werden.

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

Fake-News

→ Wann soll eine Nachricht überprüft werden? (2)

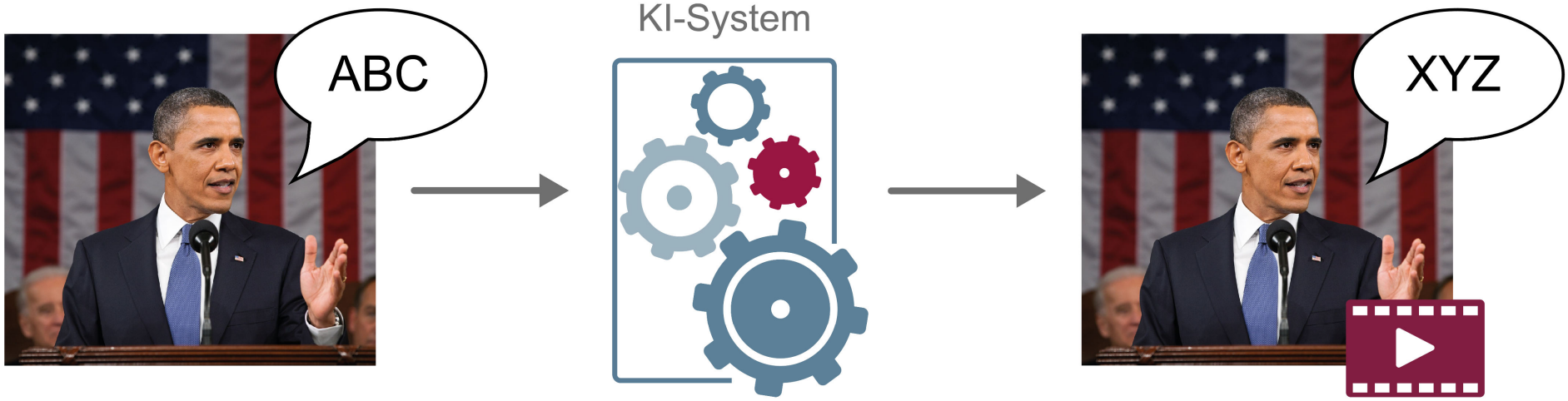
- **Immer dann, wenn ein Nutzer eine Fake News meldet.**
  - Alle Nutzer, die sich nicht sicher sind, dass eine Nachricht echt ist, melden diese an eine Stelle, die dann die Entscheidung mit Algorithmen und/oder Journalisten trifft.
  - Das können wir heute schon bei den meisten sozialen Netzwerken tun.
  - Leider ist die Anzahl der Meldungen sehr gering.

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

Deep-Fake
→ Was ist eine Deep-Fake?

- **Bildgenerierende Systeme** können überzeugend mit Hilfe von **künstlicher Intelligenz (KI)** gestellte Videos (Deep-Fake-Video) erzeugen und damit Individuen oder ganze Personengruppen ***diffamieren***, zu ***Gewalt aufrufen*** und ***Chaos anstiften***.

- Ein normaler Nutzen kann ein Deep-Fake nicht von einem echten Video unterscheiden.



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

Social Web Cyber-Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Soziale Netzwerke
- Fake-News
- **Cyber-Mobbing**
- Weitere Implikationen
- Zusammenfassung

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

Cyber-Mobbing
→ Übersicht

- Mit **Cyber-Mobbing** oder auch **Cyber-Bullying** werden verschiedene Formen der Verleumdung, Belästigung, Bedrohungen und Nötigung aber auch des Bloßstellens von Menschen oder Unternehmen mithilfe digitaler Kommunikationsmittel **im Cyber-Raum** bezeichnet.

- Typischerweise werden zum Cyber-Mobbing digitale Kommunikationsmittel wie Soziale Medien wie Facebook, Instagram, Snapchat oder YouTube, aber auch Chatsysteme wie WhatsApp, Telegram oder Signal, sowie Posts, Foren und E-Mails verwendet.

- Opfer von Cyber-Mobbing werden zum Beispiel durch Bloßstellung im Internet, permanente Belästigung durch entwürdigende Bilder oder durch Verbreitung falscher Behauptungen gemobbt.

- Die **Täter** werden bei Cyber-Mobbing auch als **Bullies** bezeichnet. Cyber-Mobbing gehört zu den Risiken im Cyber-Raum, durch die Menschen und Unternehmen gleichermaßen bedroht werden.

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

Cyber-Mobbing
→ Herausforderung (1/2)

- Das Phänomen Mobbing ist grundsätzlich nicht neu, aber durch das Internet – den Cyber-Raum – hat es eine **neue Dimension** erlangt.
- Zwar haben die meisten von uns in der Schulzeit mal erlebt, dass unangenehme Aussagen auf der Tafel geschrieben standen.
- Nur war das auf den Klassenraum begrenzt – es konnten allenfalls die anderen Mitschüler und der Lehrer diese unangenehmen Informationen lesen.
- Das Gleiche galt auch, wenn wir schlecht über unser Unternehmen gesprochen haben.
- Wenn solche Informationen jedoch im Internet stehen, können im Prinzip **alle Menschen auf der Welt** zu jeder Zeit darauf zugreifen und das Opfer hat **keine Rückzugsmöglichkeiten** vor daraus resultierenden Mobbing-Attacken.
- Dadurch, dass rufschädigende Informationen oft **im Cyber-Raum anonym** eingetragen werden können, ist die **Hemmschwelle** für die Täter viel **geringer**.

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

Cyber-Mobbing
→ Herausforderung (2/2)

- Wenn ein **Täter anonym** agiert und seinem Opfer nicht direkt gegenübersteht, bekommt er keine unmittelbare Rückmeldung für sein Verhalten und damit fehlen ihm Bewusstsein und Empfinden für das Ausmaß und die **Qualität der Verletzung**.
- Cyber-Mobbing ist für den Täter somit einfacher als Mobbing in der realen Welt. Dieser Effekt wird auch **Online-Enthemmungseffekt** genannt.
- Begünstigt wird Cyber-Mobbing dadurch, dass jemand, der anonym im Internet unterwegs ist, **kaum mit negativen Konsequenzen für sein Tun** rechnen muss.
- Doch selbst wenn eine rechtliche Handhabe zur Löschung gegeben ist, besteht das Problem, dass Informationen, die einmal im Internet stehen, nicht so leicht zu entfernen sind.
- Auch wenn es gelingt, Fotos und Beleidigungen in den digitalen Kommunikationsmitteln entfernen zu lassen, sind Opfer nicht davor geschützt, dass andere Personen die Inhalte bereits gespeichert haben und diese wieder einstellen.

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

Cyber-Mobbing
→ Unternehmen

- Problematisch für Unternehmen und insbesondere Dienstleister wie etwa Ärzte ist, dass eine Rufschädigung zu hohen Verlusten führen kann, da ungerechtfertigte negative Bewertungen unmittelbar mit einem Rückgang von Patienten oder Kunden einhergehen.
- In Deutschland ist die Meinungsfreiheit durch das Grundgesetz geschützt.
- Das bedeutet, jeder Bürger hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten.
- **Eine Zensur darf nicht stattfinden.**
- Hier ist das Internet natürlich ein gewaltiges Instrument der Meinungsäußerung, aber auch der Meinungsbildung.
- Um dies zu erhalten ist es wichtig, den Unterschied zwischen dem **Recht auf Meinungsfreiheit** und **Straftaten durch rufschädigende Informationen** zu kennen sowie auch anzuerkennen.

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

Cyber-Mobbing
→ Beispiele Bewertungsportale

- Wenn z.B. jemand in einem Bewertungsportal veröffentlicht, dass seine **Werkstatt keine gute Arbeit** geleistet hat, oder er seinen **Arzt unsympathisch** findet, dann ist dies eindeutig eine **Meinung**.
- Wenn hier jedoch kundgetan wird, dass die **Autowerkstatt einen defekten Motor eingebaut** hat oder dass der **Arzt immer falsche Medikamente verschreibt**, dann wird dadurch ein Betrug unterstellt.
- Das stellt den Tatbestand einer Rufschädigung dar und kann somit rechtliche Konsequenzen für den Einstellenden haben.
- Bei der Ahndung dieser Straftat ist jedoch die Herausforderung, dass solche Eintragungen in der Regel anonym durchgeführt werden.

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

Cyber-Mobbing
→ Weitere Begrifflichkeiten

- **Cyber Stalking**:
  Dabei ist eine verschmähte Liebe oft das Hauptmotiv. In der Regel kennen sich Täter und Opfer, es kann sich bei den gestalkten Personen jedoch auch um Prominente handeln.

- **Dissen** (von disrespect)
  wird als Sammelbegriff für diskriminierende und diskreditierende Äußerungen im Cyber-Raum verwendet.

- **Cyber-Grooming**:
  Überwiegend männliche Erwachsene tarnen sich als Kinder oder erfahrene ältere Freunde im Internet, um das Vertrauen von Kindern und Jugendlichen zu erlangen, um sie zu einem persönlichen Treffen zu überreden. Das Motiv ist sexueller Natur.

- **Happy Slapping**:
  Die Grundlage hierfür ist ein körperlicher Angriff auf meist unbeteiligte Passanten, aber es können auch Mitschüler oder Lehrer sein. Dieser Angriff wird gefilmt und dann über digitale Kommunikationsmittel veröffentlicht, um damit die Opfer der Angriffe zu erniedrigen.

- **Doxing**:
  Unter Doxing (oder auch Doxxing) wird grundsätzlich das intensive und systematische internetbasierte Zusammentragen und anschließende Veröffentlichen sensibler privater Daten verstanden, mit dem Ziel, die betroffene Person zu beeinflussen, einzuschüchtern, zu erpressen, zu mobben oder die privaten Informationen für einen Social Engineering Angriff zu verwenden. Der Name Doxing leitet sich aus den englischen Ausdrücken „Docs“ für Dokumente und „Tracing“ für Verfolgung ab.

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

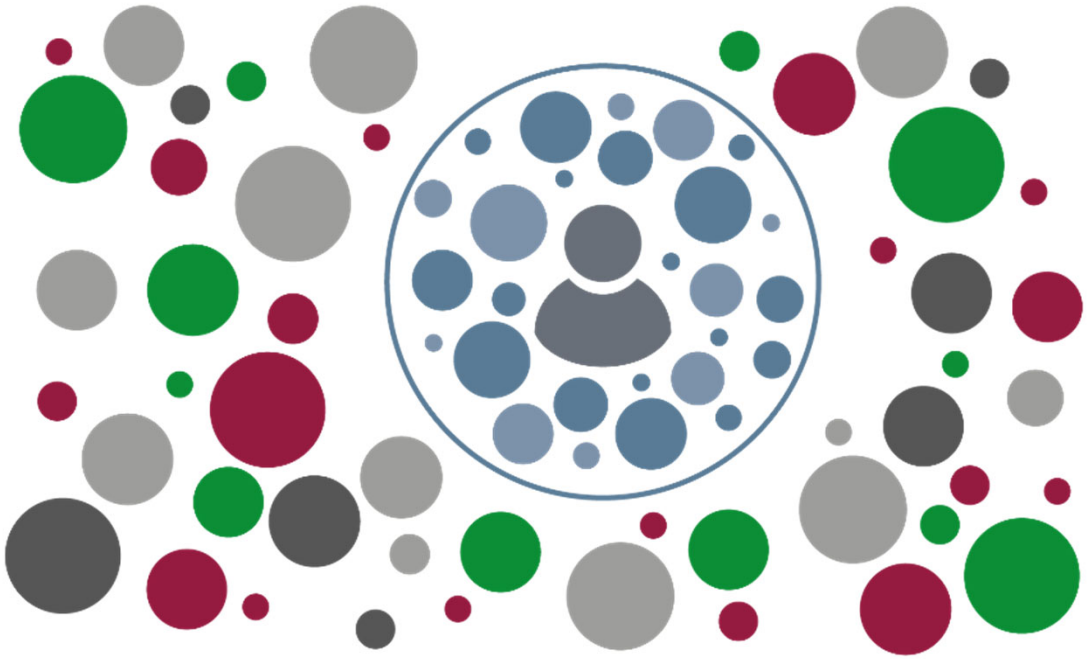
Social Web Cyber-Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Soziale Netzwerke
- Fake-News
- Cyber-Mobbing
- **Weitere Implikationen**
- Zusammenfassung

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

Weitere Implikationen
→ Filterblasen

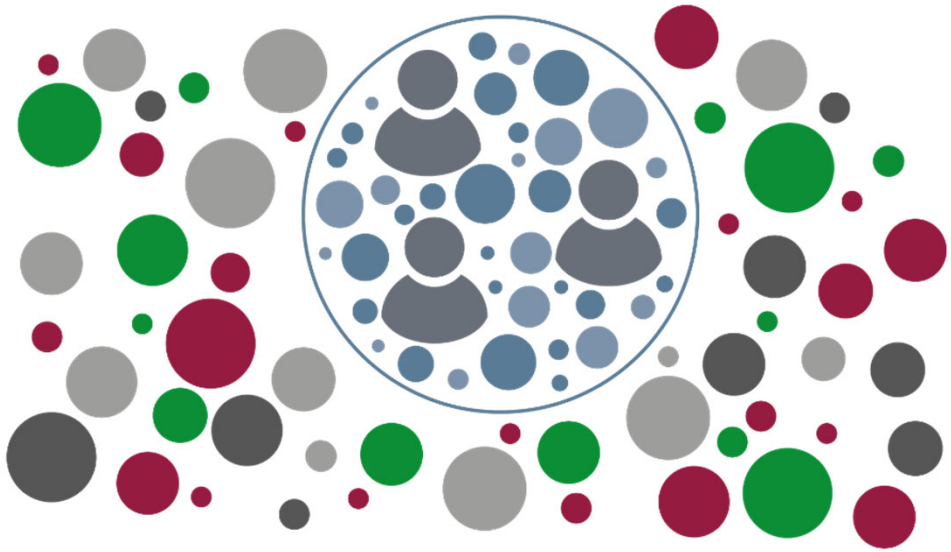
- Einem Nutzer werden tendenziell nur Nachrichten angezeigt, die mit seinen bisherigen Ansichten übereinstimmen.
  - Diese Informationen werden z.B. durch das Like- und Klick-Verhalten des Nutzers bestimmt.
  - Problem: Der Nutzer bekommt keine Nachrichten, die seinem Standpunkt widersprechen und damit eine **objektive Selbstbestimmung** ermöglichen würden.



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

Weitere Implikationen
→ Echokammern

- Phänomen: Viele Menschen in den sozialen Netzwerken neigen dazu, sich mit Gleichgesinnten zu umgeben und sich dabei gegenseitig in der eigenen Position zu verstärken.
  - **Echokammern sind Filterblasen, in denen mehrere Nutzer mit der gleichen Meinung oder Einstellung vertreten sind.**
  - Es erwächst der Eindruck, keine Minderheitsmeinung zu vertreten, sondern eine gesellschaftlich relevante Mehrheit zu sein.
  - Algorithmen der Sozialen Netze unterstützen und verstärken diesen Effekt.



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

Weitere Implikationen
→ Psychometrie (1/2)

- Psychometrie ist das Gebiet der Psychologie, das sich allgemein mit Theorie und Methode des psychologischen Messens befasst.
  - Psychometrie kann genutzt werden, um Personen mit bestimmten Eigenschaften zu identifizieren.
  - Eine Beispiel einer sollten Messung ist eine Analyse auf Facebook, die von Cambridge Analytics durchgeführt worden ist.

- Generelle Idee dieser speziellen Analyse:
  - Input: Was haben Nutzer gelikt, geshared oder gepostet
  - Output: Geschlecht, Alter, Wohnort, Hautfarbe, sexuelle und politische Ausrichtig, …

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

Weitere Implikationen
→ Psychometrie (2/2)

- Die Analyse hat ergeben: Mit durchschnittlich 68 Facebook-Likes kann vorhergesagt werden:
  - Welche Hautfarbe der Nutzer hat (95-prozentige Treffsicherheit),
  - Welche sexuelle Ausrichtung er hat (88-prozentige Wahrscheinlichkeit),
  - ob Demokrat oder Republikaner (85 Prozent).
- Aber auch Intelligenz, Religionszugehörigkeit, Alkohol-, Zigaretten- und Drogenkonsum lassen sich berechnen.
- Die Information, ob ein Nutzer Demokrat oder Republikaner ist, war bei der Verteilung von individuellen **Fake-News** während der US-Wahlen eine wichtige Information, um gezielt vorgehen zu können.

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

Social Web Cyber-Sicherheit
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Soziale Netzwerke
- Fake-News
- Cyber-Mobbing
- Weitere Implikationen
- **Zusammenfassung**

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

Social Web Cyber-Sicherheit
→ Zusammenfassung

- Social Web-Anwendungen bringen Gesellschaftsgruppen zusammen, schaffen Bürgerbeteiligungen und fördern auch Demokratie.
- Auf der anderen Seite wird es immer wichtiger, dass Lösungen umgesetzt werden, die das Einstellen von rechtlich verbotene Inhalte und mit Rechten behaftete Objekte verhindern, ohne zu zensieren.
- Negative Aspekte, wie Filterblasen und Echokammern müssen erkannt und deren Auswirkungen verhindert werden.
- Aber auch das Thema Psychometrie stellt Risiken für den einzelnen Nutzer und für die Gesellschaft dar.
- Wichtig für die Cyber-Sicherheit wird sein, dass die negativen Potentiale von sozialen Netzwerken nicht das Risiko von IT-Schäden erhöht.

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

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Social Web Cyber-Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann

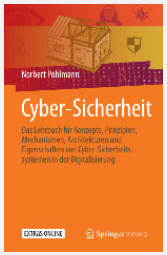
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

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

Literatur
→ Artikel / Bücher

S. Feld, N. Pohlmann, S. Spooren: „Gefahren und Risiken bei Web 2.0". Im Journal eCollaboration, Hrsg.: K. Riemer, S. Strahringer, HMD – Praxis der Wirtschaftsinformatik, dpunkt Verlag, Juni 2009
https://norbert-pohlmann.com/wp-content/uploads/2015/08/247-Gefahren-und-Risiken-bei-Web-2-0-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann, T. Urban: „Sehen heißt glauben! Aufdeckung von Webseiten Manipulation“. In Proceedings der DACH Security 2016 Konferenz, syssec Verlag, 2016
https://norbert-pohlmann.com/wp-content/uploads/2017/03/351-Sehen-heißt-glauben-Aufdeckung-von-Webseiten-Manipulation-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann „Fake-News in Sozialen Netzwerken – Das „Mitmach-Web“ hat seine Unschuld (endgültig) verloren“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 5/2017
https://norbert-pohlmann.com/wp-content/uploads/2017/10/363-Fake-News-in-Sozialen-Netzwerken-%E2%80%93-Das-Mitmach-Web-hat-seine-Unschuld-endg%C3%BCltig-verloren-Prof.-Norbert-Pohlmann.pdf

N. Demir, N. Pohlmann: „Identitäts-Check anhand sozialer Netzwerke – Das Social-Ident-Projekt“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 2/2018
https://norbert-pohlmann.com/wp-content/uploads/2018/04/374-Identitäts-Check-anhand-sozialer-Netzwerke-–-Das-Social-Ident-Projekt-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/

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