Fachhochschule
Dortmund
University of Applied Sciences and Arts

Informationssicherheit – SoSe 2023
Sicherheitsrichtlinien & Faktor Mensch

Prof. Dr. Holger Schmidt
holger.schmidt004[at]fh-dortmund.de

Fachhochschule Dortmund
Fachbereich Informatik
Professur für IT-Sicherheit, Informatik

Themen & Lernziele

Themen

- Sicherheitsrichtlinien
- Faktor Mensch in der Informationssicherheit
- Information Security Awareness

Lernziele

Die Studierenden sind in der Lage,

- Sicherheitsrichtlinien zu definieren und zu interpretieren.
- den Faktor Mensch in der Informationssicherheit einzuschätzen.
- einen Zusammenhang zwischen technischer und organisatorischer Informationssicherheit herzustellen.

Sicherheitsrichtlinien

Dieser Abschnitt basiert auf Eckert, 2023, Kapitel 1.5. Aufgrund der Präsentation als Folien und Notizen sind die Texte der Quelle typischerweise paraphrasiert.

Einleitung

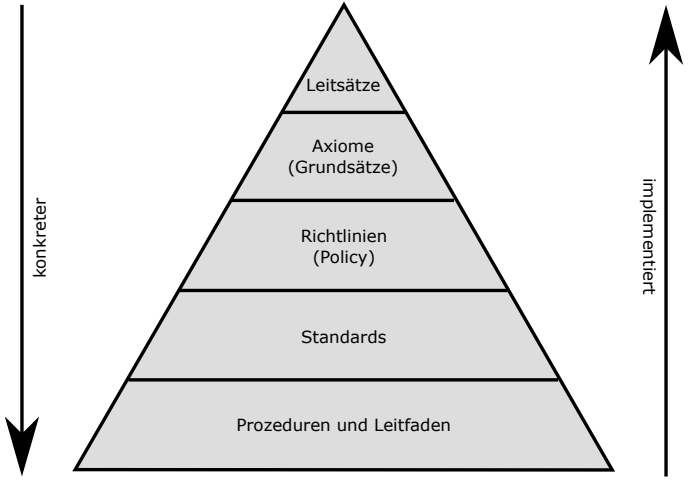


Abbildung selbst erstellt

Sicherheitsrichtlinie / security policy I

- **Sicherheitsrichtlinie (security policy)** legt **technische und organisatorische Regeln**, Verhaltensrichtlinien, Verantwortlichkeiten, Rollen und Maßnahmen fest, die zur Erreichung von Schutzzielen erforderlich sind.
- **Zugriffs- und Informationsflusskontrolle** basieren typischerweise auf
  - **Systembestimmten**, d. h. globalen, Richtlinien (mandatory policy), die von einer Einheit ausgehend für das gesamte Unternehmen festgelegt werden, und
  - **Benutzerbestimmten** Richtlinien (discretionary policy) ermöglichen die Anpassung von Berechtigungen selbsterstellter Objekte.
- Zugriffsberechtigungen häufig basierend auf **Rollen** und/oder **Attributen**

Sicherheitsrichtlinie / security policy II

- Adressieren oft **Menschen**
- Häufig **textuell** und somit **informell** definiert
- **Bereitstellung** in Unternehmen in digitaler Form für Mitarbeiter*innen z. B. via Intranet
- Regelmäßige **Kontrolle** und **mögliche Anpassung** empfehlenswert bzw. notwendig
- Kontrollierbare Umsetzung jedoch typischerweise schwierig

Beispiel – Regeln zum Passwortgebrauch[1]

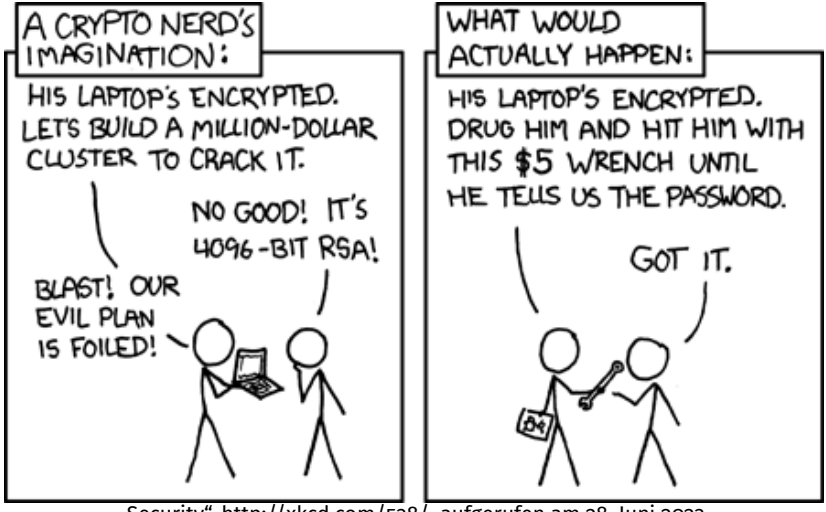
Fachhochschule Dortmund
University of Applied Sciences and Arts

- „Passwörter müssen geheim gehalten werden und nur dem Benutzer persönlich bekannt sein.“
- „Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.“
- „Passwörter dürfen nur unbeobachtet eingegeben werden.“

[1] Auszug aus https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2022/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf, aufgerufen am 28. Juni 2023

Faktor Mensch

xkcd Webcomic



„Security“, http://xkcd.com/538/, aufgerufen am 28. Juni 2023, lizensiert unter CC BY-NC 2.5.0[2]

[2] https://creativecommons.org/licenses/by-nc/2.5/

Der Faktor Mensch I

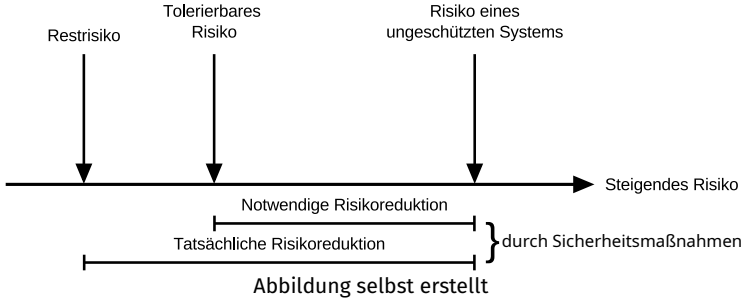


Abbildung selbst erstellt

- **Risiken** nur auf **tolerierbares Niveau** absenkbar, wenn Gegenmaßnahmen in bestimmter **Umgebung** realisiert sind
- **Mensch** als Teil der Umgebung beeinflußt essentiell Effektivität von Gegenmaßnahmen

Der Faktor Mensch II

- Menschliches Verhalten nicht zu kontrollieren; entsprechend nur **Annahmen** darüber möglich
- Mensch als **Schwachstelle** und damit Angriffsziel
- Ausnutzung menschlicher Eigenschaften zur **gezielten** Beeinflussung menschlichen Verhaltens
- So herbeigeführte „Ausnahmesituation“ verleitet häufig zu **unterbewussten Handlungen**, welche einen weitergehenden Angriff ermöglichen
- Derartiges **Social Engineering** erfordert nur **geringen Aufwand** bei typischerweise **hoher Erfolgsquote**

Aktuelle Entwicklungen bezogen auf den Faktor Mensch I

- Stetig steigende Anzahl erfolgreicher Angriffe auf den Faktor Mensch (so z. B. via **Phishing**) (Symantec, 2019)
- Phishing eher rückläufig, **Spear-Phishing** nimmt zu, dabei insb. auf kleine und mittlere Unternehmen (KMU) (seit 2013 jährlich ansteigend) (Symantec, 2019)
- Angriffe erfolgen typischerweise **online** (z. B. via E-Mail) und **offline** (z. B. via Telefon)

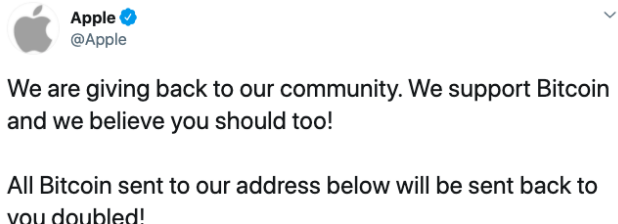
Aktuelle Entwicklungen bezogen auf den Faktor Mensch II

- Insb. am Beispiel Phishing Verlagerung von E-Mail hin zu **Social Media** erkennbar (Symantec, 2019)
- Gezielte Ausrichtung der Angriffe auf Bank- und Finanzwesen erkennbar (Proofpoint Inc., 2022)
- Social Engineering Techniken entwickeln sich fortwährend weiter und erfolgen oft in hoher Frequenz, wodurch Angriffe **schwierig abzuwehren** sind.

Twitter Bitcoin Scam

Twitter Bitcoin Scam vom 15.07.2020[3]

- 130 Twitter Konten von Prominenten (darunter z. B. Joe Biden, Bill Gates, Elon Musk) und Firmen übernommen
- In Minuten durch über 300 Transaktionen mehr als 100.000US$ eingenommen



Screenshot eines Tweet eines kompromittierten Apple Account

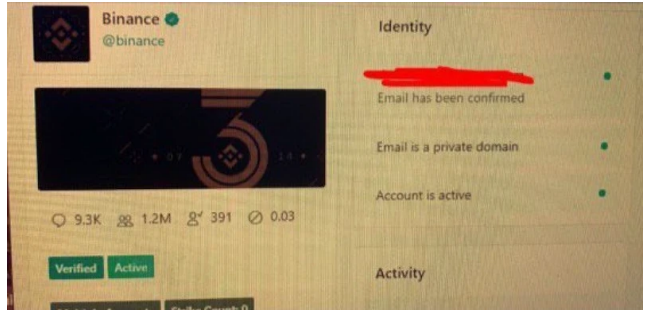
https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised

aufgerufen am 28. Juni 2023

[3]https://en.wikipedia.org/wiki/2020_Twitter_bitcoin_scam, aufgerufen am 28. Juni 2023

Hintergrund – Koordinierter Social Engineering Angriff[4][5]

- Zugangsdaten für Twitter VPN von Twitter Mitarbeiter via **Phone Spear Phishing** erlangt
- Internes Administrationswerkzeug für Twitter Konten für Zurücksetzen der Passwörter genutzt



Screenshot eines Twitter Administrationswerkzeugs

https://www.vice.com/en/article/jgxd3d/

twitter-insider-access-panel-account-hacks-biden-uber-bezos

aufgerufen am 28. Juni 2023

[4]https://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/, aufgerufen am 28. Juni 2023

[5]https://www.forbes.com/sites/louiscolumbus/2020/07/18/dissecting-the-twitter-hack-with-a-cybersecurity-evangelist/?sh=63c5ac5647df, aufgerufen am 28. Juni 2023

Hintergrund – Phone Spear Phishing[6]

- **Auswahl Twitter Mitarbeiter** über LinkedIn: Recruiter-Dienste erlauben Zugriff auf Telefonnummer
- Twitter Mitarbeiter aufgrund COVID-19 Pandemie zumeist im Home Office
- Angreifer geben sich als Twitter Mitarbeiter aus und fordern „echte“ Twitter Mitarbeiter zur Anmeldung in gefälschtem Twitter VPN auf
- **Abgreifen der Zugangsdaten** für „echtes“ (sogar 2FA geschütztes) Twitter VPN
- Angreifer haben somit über Twitter VPN **Zugriff auf Administrationswerkzeug**

[6] https://arstechnica.com/information-technology/2020/07/twitter-hackers-used-phone-spear-phishing-in-mass-account-takeover/, aufgerufen am 28. Juni 2023

Hintergrund – Übernahme Twitter Konten[7]

Fachhochschule Dortmund
University of Applied Sciences and Arts

- Angreifer nutzten Administrationswerkzeug um E-Mail-Adresse in Twitter Konten zu ändern und 2FA-Einstellungen zu widerrufen
- Daraufhin wurde die Passwörter Zurücksetzen Funktion genutzt:
  1. Telefonnummer für 2FA SMS war ursprünglich NICHT hinterlegt: Code für Zurücksetzen des Passworts ging NUR an die neue E-Mail-Adresse
  2. Telefonnummer für 2FA SMS war ursprünglich hinterlegt: Code für Zurücksetzen des Passworts ging zusätzlich per SMS an hinterlegte Telefonnummer
- Ergebnis: **Twitter Konto übernommen**, z. T. in Unkenntnis der Besitzer des Kontos

[7] https://lucky225.medium.com/the-twitter-hack-what-exactly-happened-d8740d33c1c, aufgerufen am 28. Juni 2023

Hintergrund – Forensik und Täter[8][9][10]

- FBI verhaftet drei Täter am 30.07.2020.
- Die Angreifer wurden durch Ihre Social Media Aktivitäten (OGUsers Forum, Twitter, Discord) und Transaktionen einer Crypto Währung identifiziert.
- Hohe Haftstrafen (mindestens 10 Jahre bzw. 3 Jahre bei jugendlichem Täter)

[8] https://www.wired.com/story/how-alleged-twitter-hackers-got-caught-bitcoin/, aufgerufen am 28. Juni 2023

[9] https://www.nytimes.com/2020/07/17/technology/twitter-hackers-interview.html, aufgerufen am 28. Juni 2023

[10] https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack, aufgerufen am 28. Juni 2023

Analyse

Auswirkungen:

- Integritätsverlust und Übernahme von Twitter Konten
- Monetäre Verluste (Transaktionen, Aktienkurs, etc.) und Reputationsminderung (Twitter, Betroffene)

Fehlerbehebung:

- Entfernen von Tweets, Sperrung Twitter Konten, ggf. weitere Maßnahmen

Analyse:

- Twitter Mitarbeiter **authentifizieren Telefonpartner unzureichend**
- **Fehler in Administrationswerkzeug** erlaubt Änderung E-Mail-Adresse ohne Bestätigung an vorherige E-Mail-Adresse
- Zugriff auf Administrationswerkzeug durch **viel zu große Nutzergruppe**

Faktor Mensch (Fortsetzung)

Beispiele für Angriffstechniken (auf den Faktor Mensch) I

Phishing Erlangung von Informationen (z. B. Login-Daten) auf Basis der Fälschung von E-Mails oder Websites eines Unternehmens. Auf diese Weise kann auch Malware platziert werden.

Spear Phishing Zustellung von z. B. E-Mails an ein gezielt gewähltes Opfer, welches durch das Öffnen eines Anhangs oder Links Malware installiert oder Informationen preisgibt.

Baiting / „Verlorene“ Datenträger Auslegen vermeintlich verlorener Datenträger (z. B. USB-Sticks von konkurrierendem Unternehmen), die Finder zum Öffnen innerhalb des Firmennetzes verleiten.

Beispiele für Angriffstechniken (auf den Faktor Mensch) II

Pretexting / Fake-IT-Support Anrufe durch angebliche Mitarbeiter aus der eigenen IT-Abteilung oder z. B. von Microsoft. Ziel: Anleitung zur Installation von Malware oder Deaktivierung von Schutzmechanismen.

Soziale Netzwerke Übernahme von Identitäten (z. B. Freunden oder Arbeitskollegen) zur Ausnutzung von Vertrauen bzw. Erlangung von Insider-Informationen.

Weitere Dumpster Diving (Müll durchsuchen), Shoulder Surfing („über die Schulter schauen“)

Beispiele für ausnutzbare menschliche Eigenschaften

Fachhochschule Dortmund
University of Applied Sciences and Arts

Neugierde kann zu kritischen Handlungen verleiten, die dann keinerlei äußere Einwirkung mehr benötigen.

Angst wird häufig durch das Vortäuschen einer besonders kritischen Situation (Notfallsituation) hervorgerufen und verleitet z. B. zu schadhaften Handlungen von Angestellten.

Untergebenheit / Respekt können bei Einschüchterungsversuchen via Social Engineering – z. B. beim Vortäuschen einer übergeordneten eigenen Rolle im selben Unternehmen – gezielt ausgenutzt werden.

Hilfsbereitschaft kann zur falschen Unterstützung durch Angreifer gezielt missbraucht werden.

Vertrauen aufbauen (z. B. vorgetäuschtes Anvertrauen von Informationen) dient oft der Vorbereitung von Social Engineering Angriffen.

Vgl. (Helisch & Pokoyski, 2009)

Schäden durch erfolgreiche Angriffe

- Verletzung von Schutzzielen (Verfügbarkeit, Vertraulichkeit, Integrität)
- Materieller und/oder monetärer Schaden
- Imageschaden
- Datenverlust

Security Awareness / Sicherheitsbewusstsein

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. (Wilson & Hash, 2003)

- **Security Awareness** (Sicherheitsbewusstsein) beschreibt Wissen um Angriffstechniken und Risiken.
- Sicherheitsmaßnahme zur Risikoreduktion
- Adressiert nicht nur Social Engineering (primär extrinsisch), sondern auch menschliche Versäumnisse (z. B. regelmäßige Überprüfung und Anpassung von Zugängen) oder Fehlhandlungen (primär intrinsisch)

Security Awareness Maßnahmen

- Security Awareness nur unter **Einbeziehung menschlicher Eigenschaften** herstell- und verbesserbar
- Social Engineering Risiken **nicht einzig durch technische Mittel ausreichend reduzierbar** (PricewaterhouseCoopers, 2015).
- Technische Mittel um **Minimalschutz** zu gewährleisten, z. B. Aktenvernichtung (Dumpster Diving), Sichtschutzfolien (Shoulder Surfing), USB ausschalten (Baiting)
- Verankerung von Security Awareness in Sicherheitsrichtlinien

Security Awareness Kampagnen I

- **Kampagnen** zur Steigerung der Security Awareness
- Erfüllung von Anforderungen, z. B. bei **Zertifizierung nach Standards**
- Etablierung einer **Sicherheitskultur** als Ziel von Security Awareness Kampagnen
- Konsequente **Einbeziehung von Mitarbeitern und Geschäftsführung**

Security Awareness Kampagnen II

Beispiel aus einer Awareness-Kampagne der Firma Microsoft; Foto selbst erstellt

- Security Awareness Kampagnen beinhalten häufig z. B. :
  - Schulungen / Trainings (auch als E-Learning)
  - Vorträge
  - Flyer, Anleitungen, Anweisungen
  - Plakate, Poster, Banner
  - Videos und interaktive Kampagnen im Intranet

Vgl. (Helisch & Pokoyski, 2009)

Zusammenfassung

Zusammenfassung

- Mensch als essentieller Faktor in der Systemumgebung erkannt und analysiert
- Maßnahmen zur systematischen Verbesserung der Security Awareness vorgestellt
- Richtlinien zur Einbeziehung von Menschen erklärt

Weiterführende Literatur

Weiterführende Literatur

- *IT-Sicherheit – Konzepte - Verfahren - Protokolle*, Kapitel 1.5 von Eckert (2023)
- IT-Grundschutz-Kompendium, insb. ORP und INF[11]
- *Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung* von Helisch und Pokoyski (2009)

[11] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html, aufgerufen am 28. Juni 2023

Literatur I

- Eckert, C. (2023). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (11. Aufl.). De Gruyter Oldenbourg. (Siehe S. 5, 35).
- Helisch, M., & Pokoyski, D. (2009). *Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*. Vieweg+Teubner. (Siehe S. 26, 31, 35).
- PricewaterhouseCoopers. (2015). *Turnaround and transformation in cybersecurity – Key findings from The Global State of Information Security® Survey 2016* (Techn. Ber.). (Siehe S. 29).
- Proofpoint Inc. (2022). *The Human Factor 2022 – A Proofpoint Research Report* (Techn. Ber.). https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf (siehe S. 15).
- Symantec. (2019). *ISTR24 – Internet Security Threat Report* (Techn. Ber.). (Siehe S. 14, 15).

Literatur II


Wilson, M., & Hash, J. (2003). *NIST Special Publication 800-50 – Building an Information Technology Security Awareness and Training Program*. U.S. Dept. of Commerce, National Institute of Standards; Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf (siehe S. 28).