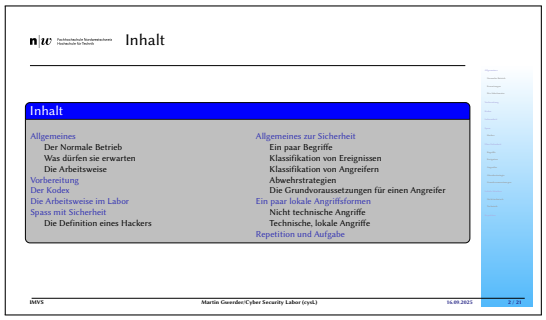


Abbildung 1: Inhaltsverzeichnis

Inhaltsverzeichnis

1 Allgemeines

1.1 Der Normale Betrieb

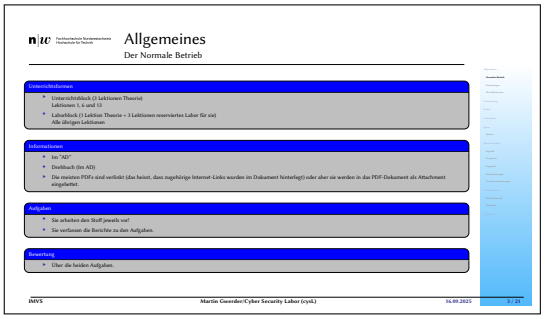


Abbildung 2: Folie “Allgemeines”/“Der Normale Betrieb”

Grundsätzlich ist das Drehbuch auf dem “AD” verbindlich. Nach diesem Dokument werden sie gemessen und danach läuft der Betrieb im Labor ab. Zusätzliche Informationen über die einzelnen Labors, sowie die Slide-Sets werden im “AD” publiziert. Sie finden dort auch alle Veranstaltungstermine und können diese ins Outlook verlinken.

Wir beginnen die Lektionen mit einem Theorieblock (3 Stunden Einführung ins Labor und vorbereitende Theorie). Die nächsten 4 Blöcke bestehen jeweils aus einem kurzen Theorieblock (ca. 1h) zu den Übungen mit anschliessender Übung.

Sie finden immer alle Informationen in den abgegebenen PDF-Slidesets. Die Slidesets sind bei Theorie-Blöcken eher umfangreicher. Bei Laborblöcken zeigen sie jeweils nur einen Rumpf, der Die Aufgabe ausweist und Links auf weiterführende Dokumentation. Es kann durchaus sein, dass ein Slideset noch vor der Lektion ergänzt wird. Für die Vorarbeit sind sie aber immer komplett.

1.2 Was dürfen sie erwarten

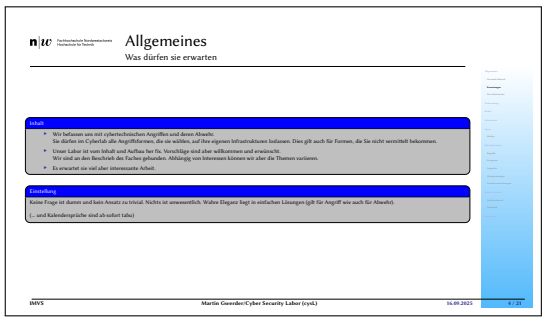


Abbildung 3: Folie “Allgemeines”/“Was dürfen sie erwarten”

Wir werden im Labor zwar den Fokus auf die Abwehr von Angriffen legen, diese machen aber keinen oder nur wenig Sinn, wenn die entsprechenden Angriffe nicht ausgeführt werden können.

Grundsätzlich gilt:

1. Sie dürfen auf ihre eigene(!) Infrastruktur jede Art von Angriffen ausführen.
2. Falls Sie dazu Software benötigen, welche sich nicht auf dem Rechner befindet, dürfen sie diese installieren.
3. Software, welche installiert wurde, muss am Ende einer Lektion wieder gelöscht sein!
4. Sie dürfen jemand anderen innerhalb des Labors angreifen. Sie benötigen aber sein schriftliches Einverständnis.

Um einen “normalen” Laborbetrieb zu gewähren wird folgende Vereinbarung empfohlen:

1. Scanning und sniffing ist immer zulässig (aktiv und passiv).
2. Jeder Angriff, direkt oder indirekt (auch auf dem gesharten Netzwerk oder einem anderen Kontext), erfordert nach wie vor das Einverständnis. Dieses kann verbal (für maximal 4h) oder schriftlich erfolgen.

1.3 Die Arbeitsweise

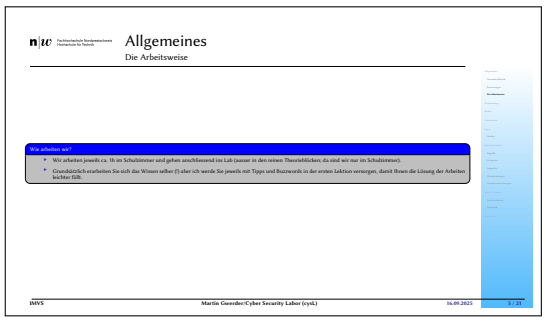


Abbildung 4: Folie “Allgemeines”/“Die Arbeitsweise”

Wir arbeiten jeweils ca. 1h im Schulzimmer und gehen anschliessend ins Lab (ausser in den reinen Theorieblöcken; da sind wir nur im Schulzimmer).

Grundsätzlich erarbeiten Sie sich das Wissen selber (!) aber ich werde Sie jeweils mit Tipps und Buzzwords in der ersten Lektion versorgen, damit Ihnen die Lösung der Arbeiten leichter fällt.

Selbstverständlich gilt hier wie immer: Es gibt keine generelle Anwesenheitspflicht. Abmeldungen werden aber gerne gesehen. Wenn Sie nicht (oder häufig nicht) Anwesend sind entfällt eine Viel grössere Aufmerksamkeit auf die Beurteilung der Arbeit. Es wird erwartet, dass Sie dort darlegen, dass Sie sich vergleichbares Wissen erarbeitet haben (oder darüber verfügen).

2 Vorbereitung

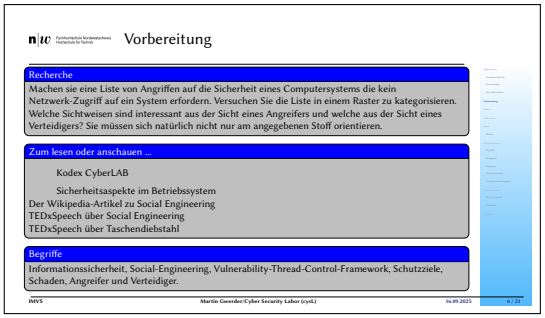


Abbildung 5: Folie “Vorbereitung”/“”

Bitte arbeiten sie jeweils die Vorbereitungs-Slide vor(!) einer Lektion durch. Sie erlauben es damit, dass alle mit einem bestimmten Vorwissen in die Lektion kommen. Dies führt zu interessanteren, abwechslungsreicheren Diskussionen.

3 Der Kodex

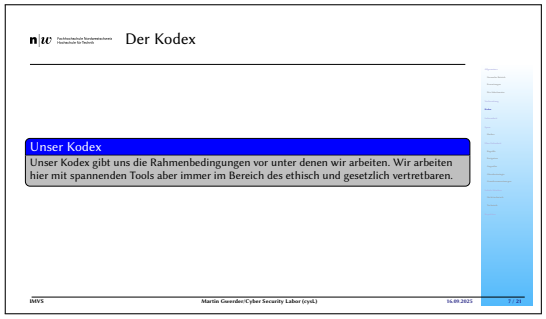


Abbildung 6: Folie “Der Kodex”/“”

Bereiten sie sich darauf vor den Kodex an dieser Stelle zu unterschreiben. Ein Muster befindet sich als Attachment in diesem Dokument.

Der Kodex deckt ihr Tun im Zusammenhang mit Cyber-Sicherheit ab. Die Schlüsselpunkte darin sind:

- Sie handeln transparent und verantwortungsbewusst.
- Sie sind bereit über ihr Tun öffentlich Rechenschaft abzulegen.
- Sie verzichten auf illegale Aktivitäten.
- Sie handeln wo immer möglich ethisch korrekt.

4 Die Arbeitsweise im Labor

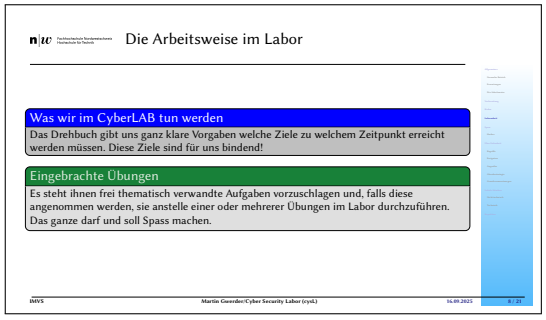


Abbildung 7: Folie “Die Arbeitsweise im Labor”/“”

Spass soll im CyberLAB immer ein zentraler Bestandteil sein. Er ist aber kein Ersatz für Arbeit. Sie müssen bereit sein die geforderten ECTS-Punkte auch zu leisten. Im Rahmen der Laborvorgaben bin ich aber gerne gewillt Anpassungen des Programms vorzunehmen. Ich bin sogar erpicht darauf ihre Vorschläge zu hören. Sie können eine Aufgabe nur für sich oder aber als Ersatz für die ganze Gruppe einbringen. Beides ist zulässig. Ein Konsens in der Gruppe können sie vorgängig versuchen herbeizuführen, ist aber nicht Voraussetzung.

5 Spass mit Sicherheit

5.1 Die Definition eines Hackers

Abbildung 9: Folie “Spass mit Sicherheit”/“Die Definition eines Hackers”

Vielleicht witzig. Machen Sie sich doch einmal Gedanken, was für ein Hacker Sie sein wollen oder sollen?

6 Allgemeines zur Sicherheit

6.1 Ein paar Begriffe

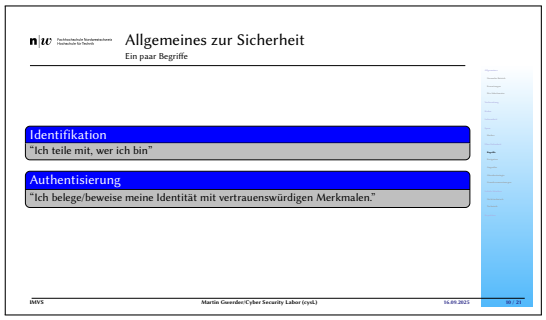


Abbildung 10: Folie "Allgemeines zur Sicherheit"/"Ein paar Begriffe"

Wenn sie zwischen Identifikation und Authentisierung unterscheiden, ist es wichtig auch über "Vertrauen" sich Gedanken zu machen. Heute ist es so, dass uns sehr häufig Betriebssysteme und Programme die Vertrauensstellungen diktieren. Wenn wir als Beispiel die Identifikation unserer Peer-Partner im Web-Browser vor Augen halten, dann sehen wir dort schön die Problematik. Der Internetexplorer identifiziert die geöffneten Webseiten am Zertifikat. Die Zertifikatsprüfung erfolgt bei verschlüsselten Verbindungen automatisch und kategorisiert in den Kategorien "Unbekannte Unterschrift", "Vertrauenswürdige Unterschrift" sowie "Vertrauenswürdige Unterschrift markiert mit erweiterter Prüfung". Technisch gesehen ist die Verschlüsselung überall von der selben Qualität. Nur die Unterschrift und deren Vertrauensverhältnis Variiert. Microsoft liefert regelmässig Sicherheitsupdates, mit denen dem Betriebssystem (und damit auch der Internet Explorer) gesagt wird, welche Unterschriften als vertrauenswürdig einzustufen sind und welche nicht. In diesem Beispiel wird also das Vertrauen von Microsoft dem Vertrauen des Benutzers gleichgesetzt. Anders ausgedrückt heisst das, dass Microsoft vorgibt, wem ein Benutzer vertraut und wem nicht.

Das hier gezeigte Beispiel liesse sich auch auf andere Programme ausweiten. So sind es beim Mozilla Firefox die Personen, die dort die Software paketieren, die das Vertrauen vorgeben. Bei Opera der Hersteller Opera und beim Safari-Browser die Firma Apple. Wir authentisieren im Web also immer über ein Vertrauen, das wir weitestgehend an Dritte abdelegieren.

Das muss nicht zwingend so sein. Bei PGP beispielsweise ist die Vertrauensstellung normalerweise aufgrund von den unterschreibenden Personen und des Vertrauens, das ich direkt oder indirekt in sie habe.

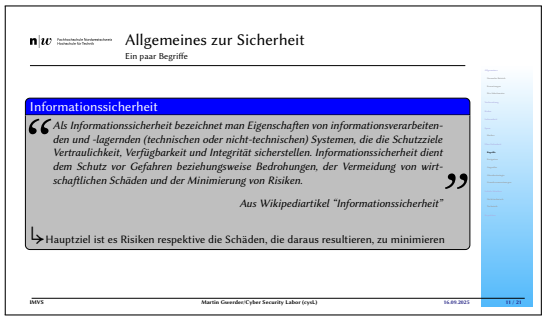


Abbildung 11: Folie “Allgemeines zur Sicherheit”/“Ein paar Begriffe”

Die Vermeidung von Schäden, die sich üblicherweise auf finanzielle Folgen eindampfen lassen, ist primäres Ziel der Informationssicherheit. Auch wenn die ökonomische Schadensminimierung im Vordergrund steht, ist sie dennoch schwer zu umreissen. Dinge wie Reputationsverlust oder die Reduktion eines Brand-Wertes können riesige finanzielle Folgen haben. Diese aber im Voraus zu beziffern ist beinahe unmöglich.

Ebenfalls zu beachten gilt es, dass Schäden nicht immer die Folge eines Angriffes sein müssen. Die Integrität eines Gebäudes wird sowohl durch eine sachgemässe Ausführung beim Bau, durch gute (oder mangelnde) Pflege aber auch durch die Stärke von seismischen Erschütterungen (im Extremfall ein Erdbeben) beeinträchtigt. Es ist also ein vielschichtiges Thema.

Im Folgenden befassen wir uns fast ausschliesslich aber mit Gefährdungen im Zusammenhang mit gerichteten oder ungerichteten kriminellen Aktivitäten von einzelnen Individuen oder von Kollektiven, die es auf die Aspekte “Vertraulichkeit”, “Integrität” oder “Verfügbarkeit” abgesehen haben.

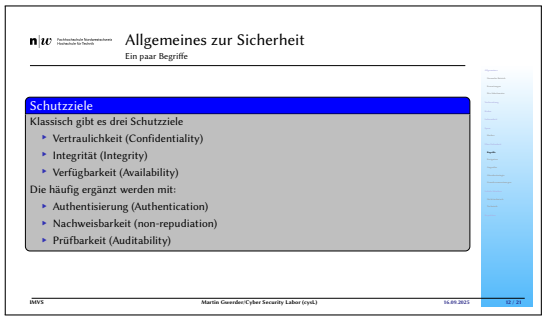


Abbildung 12: Folie “Allgemeines zur Sicherheit”/“Ein paar Begriffe”

Die traditionellen Schutzziele können auf verschiedene weisen umschrieben werden. Eine sehr Datenzentrische Umschreibung könnte wie folgt lauten:

- Vertraulichkeit (Confidentiality)
  Niemand, der nicht dazu berechtigt ist, kann auf Daten Zugreifen.
- Integrität (Integrity)
  Niemand, der nicht dazu Berechtigt ist, kann die Daten ändern.
- Verfügbarkeit (Availability)
  Alle Personen, die die technischen Voraussetzungen erfüllen, können (vorhergehende Einschränkungen berücksichtigt) auf die Daten zugreifen.

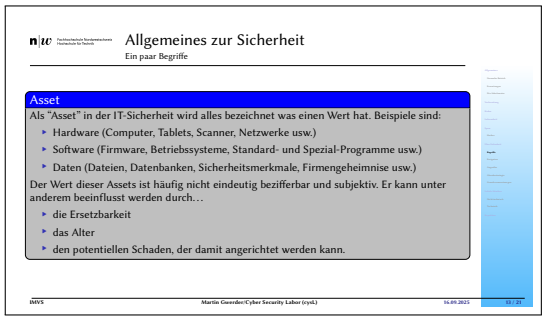


Abbildung 13: Folie "Allgemeines zur Sicherheit"/"Ein paar Begriffe"

Als "Asset" in der IT-Sicherheit wird alles bezeichnet was einen Wert hat. Beispiele sind:

- Hardware
  Computer, Tablets, Scanner, Netzwerke, Drucker usw.
- Software
  Firmware, Betriebssysteme, Standard- und Spezial-Programme usw.
- Daten
  Dateien, Datenbanken, Backups, Sicherheitsmerkmale, Firmengeheimnise usw.

Der Wert dieser Assets ist häufig nicht eindeutig bezifferbar und subjektiv. Er kann unter anderem beeinflusst werden durch…

- Die Ersetzbarkeit
- Das Alter
- Den potentiellen Schaden, der damit angerichtet werden kann.

6.2 Klassifikation von Ereignissen

Abbildung 15: Folie “Allgemeines zur Sicherheit”/“Klassifikation von Ereignissen”

Es gibt mehrere Möglichkeiten Ereignisse zu Klassifizieren. Gängigerweise werden sie aufgeteilt wie folgt:

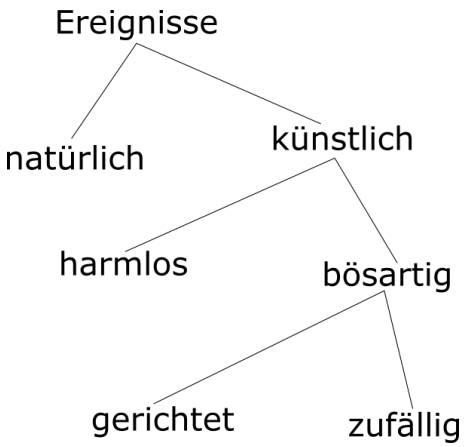


Abbildung 16: Klassifizierung von Ereignissen

Wir befassen uns im Folgenden primär mit künstlichen Attacken. Dies unabhängig davon ob sie harmlos, böswillig, gerichtet oder ungerichtet sind.

6.3 Klassifikation von Angreifern

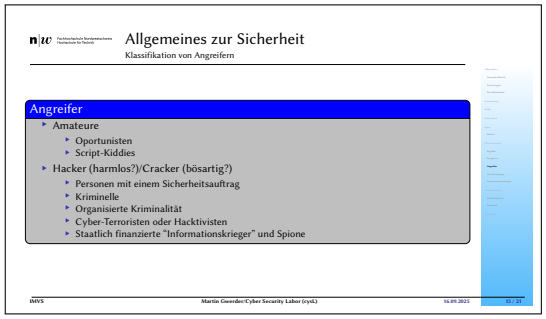


Abbildung 17: Folie "Allgemeines zur Sicherheit"/"Klassifikation von Angreifern"

Typischerweise werden Angreifer wie folgt klassifiziert:

- Amateure
  - Oportunisten
    "Es gab da gerade eine nette, kleine Möglichkeit…"
  - Script-Kiddies
    "Ich habe da ein cooles Script/ein Youtube-Video/etwas gelesen/einen Geissfuss, welches mir einen Angriff ermöglicht."
- Hacker (harmlos?)/Cracker (bösartig?)
  - Personen mit einem Sicherheitsauftrag Das wären dann alle anwesenden in diesem Kurs.
  - Kriminelle
  - Organisierte kriminalität
  - Cyber-Terroristen oder Hacktivisten
  - Staatlich finanzierte "Informationskrieger" und Spione

6.4 Abwehrstrategien

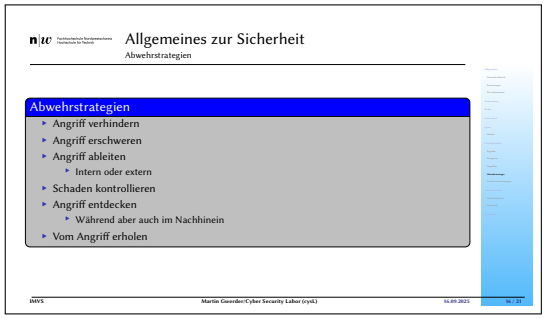


Abbildung 18: Folie “Allgemeines zur Sicherheit”/“Abwehrstrategien”

Man versucht bei der Abwehr mehrere Schutzwälle aufzuziehen. Da es die absolute Sicherheit nicht gibt ist es das Ziel möglichst kosteneffizient möglichst viele Angriffe abzuwehren, so dass die TCO-Betrachtung stimmt.

- Angriff verhindern
  Dies ist immer am Besten aber kann immer nur für bekannte Angriffe gemacht werden.
- Angriff erschweren
  Die einfachste Möglichkeit einen Angriff zu erschweren ist es Informationen zu verbergen. Dies wird häufig als ein Sicherheitsmerkmal betrachtet. In der Sicherheitsbranche gilt es aber weitläufig als akzeptiert, dass Information-Hiding Angriffe erschweren kann aber kein Sicherheitsmerkmal ist (Vergleiche hierzu “Security through obscurity”).
- Angriff ableiten
  Eine andere Möglichkeit ist es Angriffe auf Infrastrukturen abzuleiten, welche damit umgehen können. Typische Beispiele sind Honeypots.
  - Intern
  - extern
- Schaden kontrollieren
  Praktische Anwendung hier können sein:
  - Nicht benötigte Informationen zu löschen
  - Informationen unzugänglich machen indem sie auf ein Drittsystem ohne Lesezugriff ausgelagert werden.
  - Informationen geeignet ablegen (Passworte statt im Klartext in der Form von Salted Hashes ablegen).
- Angriff entdecken
  - Während
  - Im Nachhinein
- Vom Angriff erholen

6.5 Die Grundvoraussetzungen für einen Angreifer

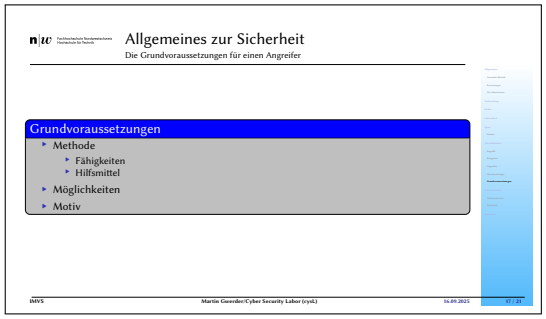


Abbildung 19: Folie “Allgemeines zur Sicherheit”/“Die Grundvoraussetzungen für einen Angreifer”

Für einen Angriff braucht es bestimmte Grundvoraussetzungen:

- Methode
  - Fähigkeiten
  - Hilfsmittel
- Möglichkeiten
- Motiv

7 Ein paar lokale Angriffsformen

7.1 Nicht technische Angriffe

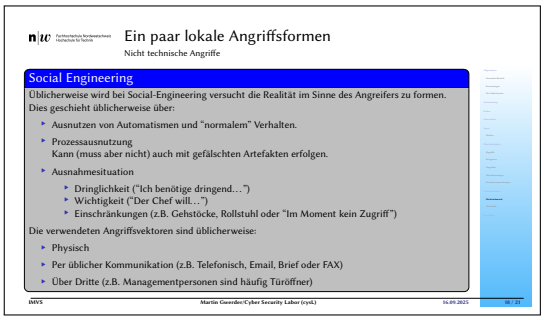


Abbildung 20: Folie "Ein paar lokale Angriffsformen"/"Nicht technische Angriffe"

Beim Social Engineeringe wird üblicherweise versucht die Realität im Sinne des Angreifers zu formen. Dies geschieht üblicherweise über:

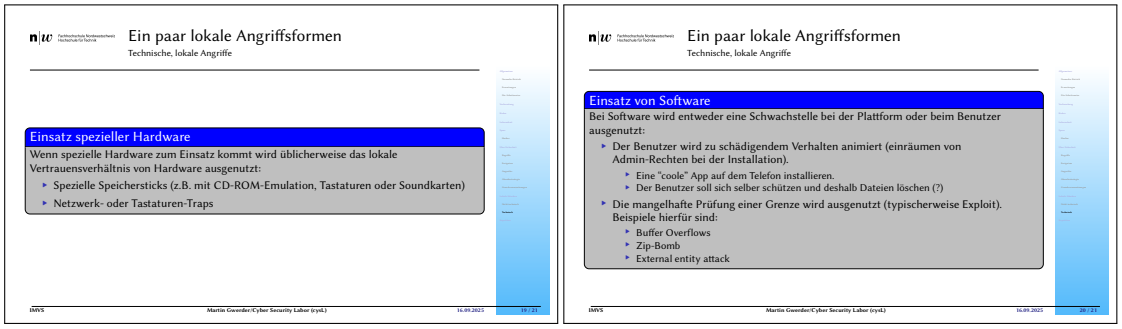
- Ausnutzen von Automatismen und "normalem" Verhalten.
- Prozessausnutzung
  Kann (muss aber nicht) auch mit gefälschten Artefakten erfolgen.
- Ausnahmesituation
  - Dringlichkeit ("Ich benötige dringend…")
  - Wichtigkeit ("Der Chef will…")
  - Einschränkungen (z.B. Gehstöcke, Rollstuhl oder "Im Moment kein Zugriff")

Die verwendeten Angriffsvektoren sind üblicherweise:

- Physisch
- Per üblicher Kommunikation (z.B. Telefonisch, Email, Brief oder FAX)
- Über Dritte (z.B. Managementpersonen sind häufig Türöffner)

Dies ist aber nicht die einzige Angriffsform. Sie können zum Beispiel versuchen eine Demokratie angreifen, indem sie demokratische Mittel (Initiative, Referendum usw.) verwenden um diese ausser Kraft zu setzen.

7.2 Technische, lokale Angriffe



(a) (b)

Abbildung 21

Folie “Ein paar lokale Angriffsformen”/“Technische, lokale Angriffe” Meistens wird der lokale physische Zugriff als Sicherheitsmerkmal betrachtet. Dies ist auch der Grund, weshalb Server und Netzwerkräume immer abgeschlossen sein sollten.

8 Repetition und Aufgabe

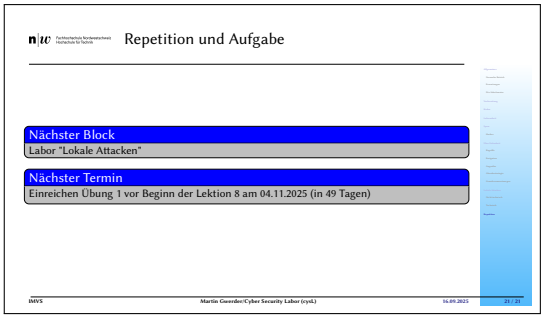


Abbildung 22: Folie “Repetition und Aufgabe”/“”