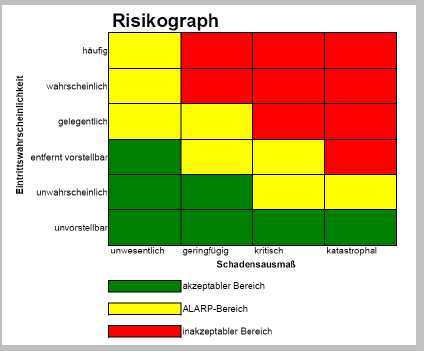
Prüfungszusammenfassung

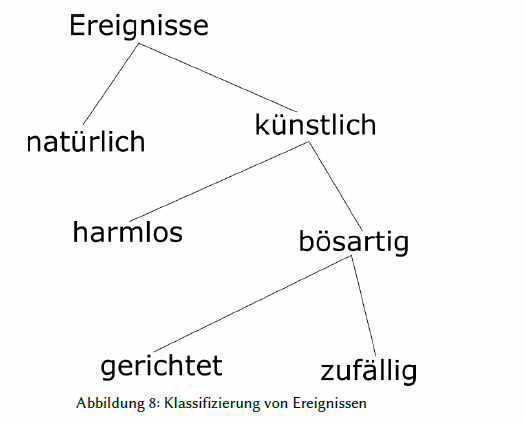
# Woche 1

* Schweizer Recht gilt immer nur in der Schweiz (Ein Problem im Internet)
  + Schweizer Recht gilt uneingeschränkt, wenn Täter, Opfer und Tatort in der Schweiz liegen
  + Wenn nur das Opfer in der Schweiz liegt, lässt sich Schweizer Recht schlecht durchsetzen
  + Wenn nur der Täter zum Zeitpunkt in der Schweiz war, ist Schweizer Recht durchsetzbar
* Obligationenrecht (OR)
  + Regelt Verträge und Verpflichtungen
  + Für das Zustandekommen eines Vertrages bedarf es nicht einer besonderen Form/Schriftlichkeit. Beispielsweise nur über Gestik (Ich lege im Supermarkt die Ware in den Korb und dann aufs Band) 🡪 Dasselbe gilt im Internet
  + Da Gestiken im Internet nicht anwendbar sind, bedarf es einer anderen expliziten Einwilligung, beispielsweise der Eingabe der Kreditkartendaten (Rechtlich umstritten)
* Fernmeldegesetz (FMG)
  + 3 ganz wichtige Grundsätze
    - Wer einen Fernmeldedienst (Datenübertragung von Dritten) erbringt, muss dies dem Bundesamt für Kommunikation (BAKOM) melden. Der Bundesrat registriert die gemeldeten AnbieterInnen von Fernmeldediensten
    - Der Bundesrat kann insbesondere für die Fernmeldedienste von geringer technischer und wirtschaftlicher Bedeutung Ausnahmen vorsehen (WLAN Router 🡪 Datenübertragung von Dritten)
    - Er regelt die Einzelheiten der Meldungen sowie die regelmässige Aktualisierung der Liste der Anbieterinnen von Fernmeldediensten
  + Der zweite Grundsatz sorgt also dafür, dass nicht alles (WLAN Router, Mailserver etc.) in einer Bürokratieorgie ausartet
* Datenschutzgesetz (DSG)
  + Grenzüberschreitende Bekanntgabe
    - Personendaten dürfen nichts ins Ausland gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil die Gesetzgebung fehlt. Die einen angemessenen Schutz gewährleistet
    - Fehlt eine solche Gesetzgebung, dürfen die Personendaten nur im Ausland bekannt gegeben werden, wenn:
      * Hinreichende Garantien durch einen Vertrag zum Schutz der Daten bestehen
      * Die Person eingewilligt hat
      * Es einen Zusammenhang zum Abschluss/Abwicklung des Vertrages gibt (Kausalzusammenhang)
      * Eine Bekanntgabe der Wahrung des öffentlichen Interesses entspricht oder eine rechtliche Angelegenheit tangiert
      * Wenn es um die körperliche Integrität (Gesundheit) der Person geht
      * Die Daten der Person durch die Person selber schon bekannt gemacht worden sind
      * Es sich beim Kunden und Verkäufer um dieselbe juristische Person handelt (Ich möchte meine eigenen Daten in Japan verarbeiten lassen)
    - Der EDÖB muss über den ersten und letzten Paragraphen (Garantien und dieselbe Person) benachrichtigt werden
  + Auskunftsrecht
    - Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob die Daten bearbeitet werden
    - Der Inhaber einer Datensammlung muss der betroffenen Person mitteilen
      * Alle über sie in der Datensammlung vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten
      * Den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorie der bearbeiteten Personen der an der Sammlung Beteiligten und der Datenempfänger
    - Das Bearbeiten von Daten durch Dritte entbindet nicht von der Auskunftspflicht
    - Die Die Auskunft ist in der Regel schriftlich und in Form eines Ausdruckes/Fotokopie kostenlos zu erteilen (Der Bundesrat regelt Ausnahmen)
    - Niemand kann im Voraus auf das Auskunftsrecht verzichten
  + Rechtsansprüche
    - Die klagende Person kann verlange, dass die Datenverarbeitung gesperrt wird, keine Daten an Dritte bekanntgegeben werden oder die Personendaten berichtigt oder vernichtet werden
    - Kann weder die Richtigkeit noch Unrichtigkeit dargetan werden, kann der Kläger das Anbringen eines Vermerks fordern
    - Die klagende Person kann verlangen, dass eine Sperrung, Berichtigung etc. oder das Urteil Dritten mitgeteilt oder veröffentlicht wird
* Urheberrechtsgesetz (URG)
  + Werkbegriff
    - Werke sind unabhängig von ihrem Wert oder Zweck, geistige Schöpfungen der Literatur und Kunst, die einen individuellen Charakter haben (Literatur, akustische Werke, Kunst, Baukunst, Fotografie)
    - Als Werke gelten auch Computerprogramme
    - Ebenfalls geschützt sind Entwürfe, Titel und Teile von Werken, sofern es sich um eine geistige Schöpfung mit individuellen Charakter handelt
  + Urheber ist die natürliche Person, die das Werk geschaffen hat
  + Verwendung des Werkes
    - Der Urheber hat das ausschliessliche Recht zu bestimmen, ob, wann und wie das Werk verwendet wird
    - Der Urheber hat zudem das Recht, weitere Werkexemplare herzustellen, zu veräussern und diese aufzuführen
    - Der Urheber eines Computerprogrammes hat zudem das ausschliessliche Recht, dieses zu verwenden
  + Rechte an Programmen
    - Wird in einem Arbeitsverhältnis bei Ausübung einer dienstlichen Tätigkeit sowie in Erfüllung vertraglicher Pflichten ein Computerprogramm geschaffen, so ist der Arbeitgeber allein zur Ausübung der ausschliesslichen Verwendungsbefugnisse berechtigt
* Sonderfälle
  + Datenschutzgrundverordnung (DSGVO): EU
  + Bundesgesetz für den unlauteren Wettbewerb (UWG): Schweiz
  + Verbraucherstreitbeilegungsgesetz (VSGB): Deutschland
    - Ermöglicht es, Privatkunden können wahlweise an Ihrem Wohnsitz oder am Sitz der Firma klagen. Das hat weitreichende Konsequenzen
* Impressumspflicht
  + Sowohl in der Schweiz als auch vielen EU Statten gibt es eine Impressumspflicht
  + Gilt typischerweise, sobald eine Seite gewerblich oder kommerziell ist
  + Ein Impressum muss leicht auffindbar sein (Maximal 2 Klicks) und sollte mindestens folgende Punkte beinhalten
    - Vornamen und Name beziehungsweise Firma
    - Adresse von Wohnsitz beziehungsweise Sitz (Kein Postfach)
    - Email-Adresse (Telefon- und Faxnummer sind meistens nicht ausdrücklich verlangt)
    - Bei Firmen: Die Rechtsform, allfällige Aufsichtsbehörden und eventuell Gerichtsstand
* DSGVO
  + Die DSGVO regelt noch zusätzliche Informationspflichten
  + Gemäss DSGVO muss jede kommerzielle Seite, die persönliche Daten verarbeitet/speichert, zusätzlich folgende Informationen bereitstellen
    - Datenschutzbeauftragten namentlich nennen – dieser muss dementsprechend ausgebildet sein (Bei Unternehmen mit weniger als 10 Personen, die Daten verarbeiten, kann der Geschäftsführer die Funktion übernehmen)
    - Die Verarbeitungstätigkeiten auflisten: Simple Aufzählung genau welche Daten, wann, wie und warum erhoben werden. Die Erhebung darf nicht beliebig erfolgen, sondern bedarf einer Notwendigkeit. Drittanbieter müssen ebenfalls eine Auflistung anbieten (z.B. Google Analytics). Daten müssen gelöscht werden, falls sie nicht mehr verwendet werden
    - Dem Benutzer die Möglichkeit geben, sein Einverständnis zurückzuziehen
  + Ferner sind sie verpflichtet:
    - Cookies zu bewilligen oder auf das absolut technische Minimum zu beschränken
    - Alle personen-relevanten Daten im Netz zu verschlüsseln
    - Nachzuweisen, wann und wo jemand wofür sein Einverständnis gegeben hat

# Woche 2

* Schutzziele (Security Goals)
  + Vertraulichkeit/Confidentiality: Vertraulichkeit, gewährleistet, dass Daten nur für befugte Entitäten (Personen, Programme oder Dienste) zugänglich sind
  + Integrität/Integrity: Integrität gewährleistet, dass Daten, Programme oder Funktionen in unveränderter Form belassen werden (Gemessen an ihrem Sollzustand)
  + Verfügbarkeit/Availability: Verfügbarkeit gewährleistet, dass eine Funktion immer dem Funktionsbezüger zur Verfügung steht
  + Weitere Schutzziele:
    - Authentizität/Authenticity: Gewährleistung von Eigenschaften wie Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit eines Objektes
    - Verbindlichkeit/Nichtabstreitbarkeit/Non Repudiation: Verbindlichkeit, gewährleistet, dass kein Abstreiten durchgeführter Handlungen möglich ist
    - Zurechenbarkeit/Accountability: Zurechenbarkeit gewährleistet, dass jede Aktion einem Handelnden eindeutig zugewiesen werden kann
* Bedrohungen (Threads)
  + Eine Bedrohung ist eine Gefahr, welche eines der Schutzziele beeinträchtigen kann
  + Typische Ursachen: Elementarschaden, Fehlbedienung, Malware, Informationspublikation über nicht-technische Kanäle, Systemausfall aufgrund einer böswilligen Handlung
  + Typische Effekte: Funktionsausfall einer Dienstleistung (DoS Attacke), Systemmissbrauch (Verborgene Daten auf einem System), Sabotage (Entlassener Mitarbeiter modifiziert eine Datenbank) oder Spionage (Dumpster Diving)
* Aktivposten (Assets)
  + Ein Aktivposten ist etwas, womit wir einen Wert verbinden. Der Wert ist häufig subjektiv (Wert kann materieller oder auch ideeller Natur sein)
* Schwächen (Vulnerabilities)
  + Als Schwäche bezeichnen wir einen Zustand oder eine Begebenheit, durch die ein Asset gefährdet sein könnte
  + Beispielsweise könnte das rostige Geländer einer Brücke als Schwäche betrachtet werden. Sollte sie nachgeben, wenn sich jemand dagegen lehnt (Bedrohung), so könnte jemand (Aktivposten) zu Schaden kommen
* Schadensausmass (Single Loss Expectancy)
  + Der Schadensausmass ist ein Wert, der die Höhe eines Schadens bemsst
  + Meistens wird ein Wert nachfolgenden Teilkriterien bemessen
    - Anschaffungswert: Was war der Neupreis
    - Alter: Alter Wein ist teurer als neuer Wein, aber alte Computer weniger als neue
    - Ersetzbarkeit/Wiederbeschaffbarkeit: Die Mona Lisa ist materiell gesehen recht wenig Wert, aber nicht wiederbeschafbar
* Eintrittswahrscheinlichkeit (Probability of Occurence)
  + Die Eintrittswahrscheinlichkeit ist ein Wert, der verkörpert, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis oder ein bestimmter Schaden eintritt. Meistens wird sie über einen bestimmten, längeren Zeitraum (z.B. ein Jahr) betrachtet
  + Normalerweise wird von einer stetigen Verteilung ausgegangen, was aber nicht immer richtig ist
* Risiko (Risk)
  + Das Produkt aus Schadensausmass und Eintretenswahrscheinlichkeit
  + Auf jeden Fall ist ein Risiko ein Ereignis/Effekt, das nur mit einer bestimmten Unsicherheit eintrifft
* Risikostrategie (Risk Strategy)
  + Vermeidung: Ich fahre nicht Auto
  + Risikoreduktion: Ich fahre nur Auto, wenn es wirklich unbedingt sein muss
  + Risikooptimierung: Ich vermeide die gefährliche Kreuzung XY
  + Risikotransfer: Risiko? Kein Problem! Ich habe eine Versicherung!
  + Festhalten an einer Risikostruktur: Ich bin schon immer hier durchgefahren und sehe keine Möglichkeit, es besser zu machen
* Risikograph
  + Bennen einzelner Risiken mit einer ID und Eintragen
  + Die Risiken im inakzeptablen roten Bereich müssen gesenkt werden, solange bis sie in den grünen, akzeptablen Bereich fallen
  + Nicht senkbare Risiken werden im ALARP Bereich belassen (As Low as Reasonably Possible)
  + 

# Woche 3

* Angriffe
  + 
* Angreifer
  + Amateure
    - Opportunisten
    - Script-Kiddies
  + Hacker (Harmlos)/Cracker (Bösartig)
    - Personen mit einem Sicherheitsauftrag
    - Kriminelle
    - Organisierte Kriminalität
    - Cyber-Terroristen oder Hacktivisten
    - Staatlich finanzierte Informationskrieger und Spione
* Abwehrstrategien
  + Angriffe verhindern: Gilt nur für bekannte Angriffe
  + Angriffe erschweren: Erschweren von Angriffen oder verstecken von Information (Security through Obscurity)
  + Angriffe ableiten:
    - Intern, offensichtlich in einen Honeypot
    - Extern via Flood-Shielding, z.B. durch Akamei
  + Schaden kontrollieren
    - Nicht benötigte Informationen löschen
    - Informationen unzugänglich machen indem sie auf Drittsysteme ohne Lesezugriff ausgelagert werden
    - Informationen geeignet ablegen (Passworte statt im Klartext in Form von Salted Hashes ablegen)
  + Angriff entdecken
    - Während
    - Im Nachhinein
  + Von Angriffen erholen
* Nicht-technische Angriffe
  + Nicht technische Angriffe sind Angriffe, die ein Schutzziel beeinträchtigen können und als Ziel nicht eine technische Anlage haben
  + Beispiele für Ziele:
    - Menschen (via Social Engineering)
    - Prozesse (z.B. via Dumpster Diving)
    - Zustände (z.B nicht passwortgeschützte Webablage)
  + Dumpster Diving
    - Wir sprechen von Dumpster Diving, wenn vertrauliche Informationen über Abfall, Altpapier, ausrangierte Hardware oder vergleichbare Kanäle organisiert wird
    - Eine Sonderform des Dumpster Diving ist, wenn mittels eins Webarchives in der Vergangenheit publizierte, heute vertrauliche Informationen beschafft werden
  + Spying und Eveasdropping
    - Wir sprechen von Spying, wenn Informationen beschafft werden, indem Beobachtungen aungestellt werden, ohne dass Entitäten manipuliert werden. Die Beobachtungen können visueller, akustischer, technischer oder anderer Natur sein
    - Spying kann passiver (Richtmikrofon) oder aktiver Natur (Man in the Middle) sein
    - Eavesdropping ist eine Art von Spying. Wir sprechen von Eavesdropping, wenn Informationen über das Mitschneiden von legitimen Datenflüssen beschafft werden
  + Social Engineering
    - Impersonation: Vorspiegelung von Personen mit besonderem Vertrauensbezug, z.B. Supportmitarbeiter oder Chef
    - Tailgating: In einem Rollstuhl steigen, damit Personen die Türe aufhalten
    - Phishing/Spear Phishing/Vishing/Whaling: Via Email/Telefon Personen manipulieren (zielgerichtet oder gestreut)
    - Popup Fenster: 1456 Probleme auf ihrem System gefunden. Klicken Sie hier, um diese zu lösen
    - «Interessante Applikationen» z.B. wer zuletzt auf deinem Facebook Profil war 🡪 Trojaner
    - Hoaxing: Mittels Witzen/unwahren Aussagen eine Person zum eigenen Vorteil beeinflussen (Mach doch deinen PC einfach selber kaputt)
  + Arbeitsmethoden beim Social Engineering
    - Dringlichkeit
    - Autorität
    - Vertraulichkeit
    - Vertrautheit (Meist über Impersonation)
    - Schuldgefühl (Quid pro quo/Piggybacking/Tailgating)
    - Gier oder Faulheit (Baiting)
  + Angriffskanäle
    - Email: Massenangriffe
    - Telefon/VoIP): Anrufen und loslügen
    - Social Media: Hey ich kenne dich vom letzten Hasenzüchtertreffen
    - SMS/Whatsapp/Chat: Auf ihrem Konto sind verdächtige Aktionen festgestellt worden
    - Brief: Sie haben gewonnen
    - Direkt: Hey leist Du mir Geld
  + Begriffsverwirrung beim Social Engineering
    - Phishing: Ursprünglich Password Harvesting und Fishing / Vishing (Phishing over VOIP)
    - Spear Phishing oder Spearing: Phishing auf einzelne Personen oder kleine Zielgruppen (Supporter) mit gerichteten, professionellen Nachrichten
    - Whaling: Phishing auf grosse Fische (CEO, CTO etc.)
  + Gegenmassnahmen zu Social Engineering
    - Ausbildung & Sensibilisierung von Mitarbeitern
    - Etablieren von festdefinierten Prozessen, welche aber eine Ausnahmebehandlung unter dem 4 Augen Prinzip ermöglichen

# Woche 4

* Technische Angriffe
  + Klassifikation von technischen Angriffen
    - Nach Schutzziel (CIA)
    - Nach Strategie
    - Nach Schweregrad des potentiellen Schadens
    - Nach Wahrscheinlichkeit
    - Nach Komplexität
  + Gegenmassnahmen gegen technische Angriffe
    - Zugriff auf System limitieren(Verhindern)
      * Physisch
        + Bauliche Massnahmen
        + Festplatten verschlüsseln
        + Sensibilisierung und Befähigung der Mitarbeiter
      * Via Netzwerk
        + Netzwerke mit Firewalls absichern
        + Sensible Daten verschlüsseln
      * Lokal auf dem System
        + Sandboxes
        + Sichere Entwicklungssysteme und Laufzeitumgebung verwenden
        + Benutzerkonten mit eng umgrenzten Rechten verwenden
    - Angriffsfläche geringhalten (Erschweren, Kontrollieren)
      * Software patchen
      * Veraltete, unsichere oder unbenutzte Software entfernen
      * Aktive Inhalte deaktivieren
    - Schadaktivität erkennen (Entdecken)
      * Anti-Malware verwenden
      * Protokollierung
    - Potentiellen Schaden geringhalten (Ableiten, Erholen)
      * Versicherung
      * Sicherungskopien erstellen
      * Diversifikation bei den Sicherheitsmerkmalen
      * Sensible Daten signieren
  + Allgemeines über Attacken
    - Reconnaissance: Auskundschaften und Kategorisieren von Informationen. Festlegen der Strategie. Geringes Risiko
    - Exploitation: Eigentlicher Angriff, um Zugriff zu erlangen, sprich die heisse Phase
    - Reinforcement: Etablieren weiterer Zugänge auf das System (Vertikal) oder auf andere Systeme (Horizontal)
    - Covering Tracks: Aufräumen der Spuren. Hätte unüblich, da meistens à la «Dash and smash» gearbeitet wird
  + Angriff (Distributed-) Denial of Service
    - Ziel: Entfernen eines Systems/Ziel, sei es vorübergehend via Überlastung (DDOS) oder auch längerfristig (z.B. Löschen der Datenbank via SQL Injection)
    - Typische Attacken
      * Lander Attacke (Hungert Network Sockets aus)
      * Smurf-Attacke (Effiziente Überlastung des Netzwerks via Reflektorangriff)
      * SQL Injection: Zerstören von Datenbankinhalten
      * Quine-Files: Füllen von Speicher oder Disk
  + Angriff Man in the Middle
    - Bei der Man in the Middle Attacke (Auch Skimming genannt) geht es darum, dass ein Dritter sich in eine Konversation einklinkt. Normalerweise lässt sich diese Attacke durch Mutual Authentication verhindern
    - Ein Grossteil aller staatlich gesponserten Programme greift auf MITM zurück
    - Beispiel: Bankautomat mit a.) präparierter Kartenlesen b.) präparierte Tastatur und c.) zusätzliche Kamera
  + Angriff (Cache-) Poisoning
    - Bei (Cache-) Posoning geht es normalerweise darum, mittels falscher Information Datenströme umzuleiten
    - Beispiel: DNS Poisoning, ARP-Spoofing/Poisoning, DHCP-Poisoning oder HPKP Extortion mit nachfolgender Erpressung
  + Angriff Erpressung
    - Heute typischerweise durch sogenannte Ransomware implementiert (Zahlung mit Botcoins). Auch via Dumpster Diving oder Aufkauf von alten Festplatten mit nachfolgender Aufarbeitung und Erpressung
  + Angriff Privilege Escalation
    - Bei der Privilege Escalation werden typischerweise Sicherheitsbarrieren umgangen. Dies erfolgt durch Übernahme von Rechten hochprivilegierter Prozesse oder durch das Überwinden von Sicherheitsbarrieren
    - Beispiel: Buffer Overflow
  + Webbasierte Angriffe
    - Webbasierte Angriffe werden heute häufig in der Reconaissance Phase in Zusammenhang mit Phishing Mails verwendet, um glaubwürdig an Informationen oder Passworte zu kommen
    - Beispiele: Drive by Infektionen, XSS oder SQL Injection 🡪 OWASP Top 10

# Woche 5

* Indikatoren
  + Zwei Typen
    - Indikatoren für einen Angriff (IOA)
    - Indikatoren für eine Kompromittierung (IOC)
  + Grundsätzlich ist nicht ganz klar, ab wann man von einem Indikator für einen Angriff spricht
  + Beide Typen können überschneidend sein, wenn beispielsweise plötzlich weniger Ressourcen im Cluster zur Verfügung stehen (DDOS Angriff vs. Absaugen von Daten)
* Indikatoren für einen Angriff
  + Versagen eines Dienstes oder Zerstörung eines Assets
  + Geänderte Leistung eines Subsystems
  + Geändertes Verhalten eines Systems oder Subsystems
* Indikatoren für eine Kompromittierung
  + Andere Zustände eines Systems oder Subsystems, beispielsweise neue Dateien oder Dateirechte
  + Geänderte Leistung eines Subsystems, beispielsweise merklich höhere CPU Grundlast und höhere IO
  + Geändertes Verhalten eines Systems oder Subsystems
  + Wertänderung von Assets durch externe Einflüsse: Aufgrund geleakter Informationen kann beispielsweise die Konkurrenz schneller mitziehen
  + Wichtig: IOC sind ein rein reaktives Mittel, da der eigentliche Angriff schon stattgefunden hat
* Monitoring als Angriffsdetektion
  + Typische IOA
    - Logs 🡪 Senden an einen Logserver und dortige Auswertung. Logs sind so sichergestellt, falls das aktuelle System sie vernichten würde. Erkennung von systemübergreifenden Phänomenen möglich
    - Fehlschlagende Loginversuche 🡪 Bruteforce Attacke
    - Anormale Aktivitäten
  + Typische IOC
    - Vorhandene Files mit SUID Flags
    - Treiber, deren Prüfsumme unbekannt sind 🡪 File Integrity Monitor (FIM)
* Intrusion Detection System
  + Ein Intrusion Detection System (IDS) untersucht Informationsquellen nach IOCs und IOAs. Ist ein System ein IIntrusion Prevention System (IPS), dann wurde zur Detektionsfunktionalität noch die Möglichkeit hinzugefügt, Einbrüche zu unterbinden. Das kann beispielsweise im Sinne einer Query basierten Web-Application-Firewall erfolgen
  + Neuerdings werden auch Unified Thread Management (UTM) Systeme verwendet, welche alle Informationen zentral analysieren und einen einzigen Endpoint managen
* Honeypot als Angriffsdetektion
  + Ein Honeypot ist ein System oder Dienst, der für einen Angreifer attraktiv aussehen soll, aber nicht produktiv genutzt wird. Aktivität auf einem solchen System kann deshalb augenblicklich als hochgradig verdächtig eingestuft werden
  + Überdies erlaubt es ein guter Honeypot, die Interessen des Angreifers zu erkennen
* Tarpit als Angriffsdetektion
  + Tarpits sind ganz normale Dienste oder Geräte. Das Besondere an Ihnen ist, dass sie bei verdächtigen Aktionen versuchen, den Angreifer möglichst lange bei Laune zu halten. Sie werden deshalb auch als «sticky Honeypots» bezeichnet
  + IP Level Tarpit, welche DHCP Anfragen mit künstlichen Geräten auffüllt. Man weiss dann nicht mehr, wie viel Systeme effektiv im Netzwerk sind – 10 oder wirklich 200?
  + SMTP Tarpits, welche ungefragt schon zu früh senden (UBE). Diese Sender hält man dann mit diversen Möglichkeiten hin (Temporary Problems, please try later etc.)
  + Harvester Tarpits, welche Informationen oder Emailadressen sammeln. Diese lässt man dann künstlich im Kreis laufen oder generiert ihnen dynamisch Informationen, um sie hinzuhalten und abstürzen zu lassen