Physische (IT) Sicherheit

ITSI 3XHIT

Jürgen Brandl & Christoph Roschger

> *Die größte Verwundbarkeit ist die Unwissenheit.*
>
> Sunzi (um 544 - 496 v. Chr.)

Physische Sicherheit und IT-Sicherheit

“Wenn ich physischen Zugang zu einem System habe, ist Game-Over”. Mit wenigen Ausnahmen ist es es nicht möglich ein technisches System vor einem Angreifer zu schützen, welcher direkt mit der Hardware und nicht über eine technisch Schnittstelle darauf zugreifen kann. Beispiel hierfür ist, dass etwas selbst mit Supercomputer unknackbare Festplattenverschlüsselung durch eine “Cold-Boot-Attack”[1] ausgehebelt werden kann, sollte der Angreifer den so geschützten Laptop in die Hände bekommen.

Dementsprechend ist es wichtig zu verstehen, dass IT-Sicherheit sich nicht nur auf Software beschränkt oder die Konzeption sicherer Netzwerke, sondern auch den Schutz wichtiger Assets vor Diebstahl, Manipulation und Sabotage. Viele Konzepte aus der physischen Sicherheit lassen sich auch auf IT-Sicherheit anwenden und wir bedienen dieser Ideen, um abstrakte Strategien auf leicht verständliche Art zu vermitteln.

[1] https://www.youtube.com/watch?v=E6gzVVjW4yY

Ziele sicherer Systeme

Ist es das alleinige Ziel von “Sicherheit” es einem Angreifer komplett unmöglich zu machen zB in ein Gebäude einzudringen oder ein bestimmtes Fahrrad zu stehlen, so muss man entweder einen immensen Aufwand in Kauf nehmen, und selbst dann bleibt immer ein gewisses Restrisiko bestehen: Absolute Sicherheit kann in der Praxis nie gewährleistet werden! Dies ist aber auch nicht unbedingt der Anspruch; die einzelnen Zielsetzungen sind hier vielschichtiger und müssen gesondert voneinander betrachtet werden:

- **Deter.** Sichere Systeme können schon alleine durch Ihren Abschreckungseffekt erfolgreich sein: Ein mit ein wenig Aufwand knackbares Fahrradschloss kann schon ausschlaggebend sein, wenn direkt daneben ein deutlich teureres Fahrrad mit vergleichbarem Schloss geparkt ist.

- **Detect.** Sicherheitsmassnahmen müssen nicht unbedingt einen Angriff physisch verhindern – oft genügt es, den Angriffsversuch zu erkennen und zum Beispiel eine Alarmsirene zu starten.

- **Delay.** Ebenso können Sicherheitsmaßnahmen, die einen Angriff deutlich aufwändiger machen, sinnvoll sein, obwohl der Angreifer sie bei Bedarf überwinden könnte. Während Türschlösser von Wohnungstüren im Prinzip immer knackbar sind (mit entsprechenden Metallbohrern), kann der benötigte Aufwand hier stark variieren.

- **Respond**. Werden Sicherheitsvorfälle erkannt, so sollte auch adäquat darauf reagiert werden. Ein typisches Problem stellt hier die sogenannte *Alert Fatigue* dar: Andauernde (falsch positive) Alarme führen bei Menschen häufig zu einem Nachlassen der Aufmerksamkeit und schlussendlich dazu, dass diese Alarme ignoriert werden. Dies kann von einem Angreifer ausgenutzt werden, indem er solche Fehlalarme bewusst produziert und seinen Angriff dann in diesem selbst verursachten “Rauschen” versteckt.

Wichtig ist, dass für alle vier gesorgt sein muss: Ohne **Abschreckung** kann etwa ein lohnenswertes Ziel so viele Diebe auf sich ziehen, bis einer erfolgreich ist. Hat man keinen Weg einen Angriff zu **erkennen**, hat ein Dieb (im Fahrradkeller etwa) unbegrenzt Zeit ein Schloss zu knacken. Sollte der Dieb nur aufsteigen und davonradeln können, so reicht die **Zeit** nicht zu reagieren und sollte es keine **Reaktion** geben, wenn jemand versucht etwas zu stehlen, so wird es auch nicht verhindert.

Perimeter

Der Perimeter (wörtlich übersetzt “Umfang”) bezeichnet die äußere Grenze der zu schützenden Gebäude bzw. Systeme. Ein gewisses Mass an Sicherheit am kann hier zum Beispiel durch örtliche Gegebenheiten wie eine erhöhte Lage, weite ungestörte Sichtbarkeit, umgebendes Wasser oder aber auch Mauern und Zäune gegeben sein.

Zwischen den Perimetern von miteinander verfeindeten Staaten oder Gruppen (also im Grenzland) werden manchmal sogenannte *Demilitarisierte Zonen* eingerichtet. Das sind Gebiete, die nur zivil genutzt werden dürfen und auf denen Militaer weder bewegt noch stationiert werden darf. Demilitarisierte Zonen fungieren somit als *Puffer* zwischen den einzelnen Gebieten und sollen für Stabilität sorgen, da sie direkte Kontakte bzw. Übergriffe zwischen den beiden Parteien verhindern sollen. In der Praxis werden solche Zonen und deren Einhaltung oft durch Dritte wie zum Beispiel die UN überwacht.

In der Netzwerktechnik bezeichnet eine DMZ analog hierzu den Bereich zwischen zwei Netzen, meist einem internen geschützten Netzwerk und dem Internet:

Wikipedia (https://de.wikipedia.org/wiki/Demilitarisierte_Zone_(Informatik):)

Eine **Demilitarisierte Zone** (**DMZ**, auch *Demilitarized Zone*) bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.

Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z.B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste (Bastion Hosts mit z. B. E-Mail, WWW o. ä.) gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen von außen geschützt werden.

Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnerverbundes sowohl dem WAN (Internet) als auch dem LAN (Intranet) zur Verfügung zu stellen.

Ihre Schutzwirkung entfaltet eine DMZ durch die Isolation eines Systems gegenüber zwei oder mehr Netzen.

Defense in Depth

Im Deutschen auch “Zwiebelschalenmodell” genannt, bezeichnen Sicherheit nicht als eine eine Lösung für ein Problem zu sehen, sondern als eine Kombination von Maßnahmen, die alle zusammen ineinandergreifen. Anhand von einer typischen mittelalterlichen Burg kann man zum Beispiel verschiedene Sicherheitsmassnahmen beobachten: Umgeben von einem Berg, Hügel oder weitläufigen Feldern haben wir einen Perimeter, der jeden der sich nähert von weitem erkennbar macht, ein Burggraben welcher schwer mit Pferd oder Rüstung zu durchqueren ist, Mauern nur mit hohem Aufwand zu erklimmen und mehrer voneinander getrennte Innenhöfe verhindern schnelles Vordringen.

Für sich allein gesehen, würde etwa eine Mauer oder ein Burggraben nur wenig Schutz bieten aber die Kombination all dieser Maßnahmen sorgen für einen hohen Aufwand (an Männern, Material, Zeit) beim Angreifer, während sie dem Verteidiger selbst in Unterzahl eine Chance zum Sieg ermöglichen.

tl;dr: Wie in wohl jedem Tower Defense Spiel

Kameras

Überwachungskameras dienen (neben einer Abschreckungsfunktion) dazu, Angriffe sichtbar zu machen und damit “in Echtzeit” zu erkennen. Eine typische Problemstellung ist hierbei, wie Kameras für eine gegebene Grundfläche platziert werden müssen, um Sichtbarkeit in alle

Ecken und Winkel zu gewährleisten, während natuerlich aus Kosten- und Effizienzgründen nur so wenige Kameras wie möglich verwendet werden sollen. Dieses Problem nennt sich im Englischen das *Art Gallery Problem* und lässt sich mit Mitteln der algorithmischen Geometrie formal beschreiben. Es existieren hier auch verschiedene Algorithmen zur Ermittlung sinnvoller Kamerapositionen.

In der IT-Sicherheit finden sich hierzu analoge Fragestellungen: Durch die Auswertung bzw. das Monitoring von Eventlogs, Anwendungslogs, Netzwerklogs, usw. könnten wohl die allermeisten Angriffe in der Theorie erkannt werden, da bei einem modernen Betriebssystem bzw. in einem Netzwerk praktisch alle Aktionen irgendwo Spuren hinterlassen. Jedoch kann durch übermäßiges Logging eine regelrechte Datenflut entstehen, sodass sich die eigentliche Frage stellt, auf welche Quellen man zur Erkennung von Angriffen zurück greift, und auf welche nicht.

Alarme

Jede Art von sicheren System ist darauf angewiesen, dass Unregelmäßigkeiten von Menschen geprüft und eventuelle Fehlalarme als solche erkannt werden. Übertrifft die Anzahl der Fehlalarme jene der gemeldeten Vorfällen, so tritt beim Personal schnell eine “alert fatigue” auf. Besonders gefährlich ist diese etwa in Krankenhäusern, wo medizinisches Personal oft mit mehreren hundert Alarmen am Tag konfrontiert wird, von denen aber jeder wenn ignoriert potentiell tödliche Konsequenzen haben kann.

Zugangssicherheit

Der Begriff Tail-gating beschreibt das Überwinden von Zugangssperren, indem man unauffällig hinter einer anderen autorisierten Person diese durchschreitet. Am häufigsten betrifft das Tueren, fuer welche man eine Zutrittskarte benoetigt: Bevor die Tuer hinter einer anderen Person zufällt, versucht hier ein Angreifer noch schnell diese zu durchschreiten.

Vereinzelungsanlage ist eine Möglichkeit sicherzustellen, dass Personen nur einzelnen einen bestimmten Punkt passieren, etwa ein Drehkreuz oder eine nur für wenigen Sekunden geöffnete Glaswand. Dies passiert meistens auch dort, wo Zutrittsberechtigungen in elektronischer Form kontrolliert werden (Kartenlesegeräte, Tickets,...). Abgesehen von Unternehmen mit hohen Sicherheitsanforderungen, finden sich solche auch in Zoos, bei Skiliften oder auch auf öffentlichen Toiletten.

RFID

RFID ist eine Technologie, welche viele Anwendungen findet. Eine der unauffälligsten aber auch häufigsten ist der eingenähte Diebstahlschutz in Kleidung oder teuren Gegenständigen in Läden.

RFID funktioniert über eine Antenne, welche bei empfangen eines Funksignals genug Strom erzeugt, um einen Schaltkreis anzusteuern und eine Antwortsignal zurückzusenden.

RFID/NFC wird auch in Form von Zutrittskarten oder Token eingesetzt. Hierbei wird jeder Karte einen eindeutige UID vergeben und diese mit mehreren Datenblöcken beschreiben. Diese können auch in verschlüsselter Form gespeichert werden, um eine Klonen unmöglich zu machen. Die Sicherheit hängt hierbei maßgeblich von der Qualität der eingesetzten Verschlüsselung ab.

Angriffe auf Signale:

- **Replay.** Bei einem Replay-Angriff wird ein Signal - etwa das zum Entsperren eines Autos - aufgenommen und nochmal abgespielt. Replay Attacken werden verhindert, indem man mit jedem neuen Paket eine fortlaufende oder eindeutig, zufällige Nummer gibt.

- **Man-In-The-Middle.** Bei MITM-Angriff hört der Angreifer eine Kommunikation ab und kann als Zwischenstation diese in manchen Fällen auch manipulieren. Dies wird verhindert indem Kommunikation nur verschlüsselt stattfindet und beide Seiten sich gegenseitig authentifizieren.

- **Relay.** Bei einem Relay-Angriff wird eine Kommunikation vom Angreifer hergestellt, etwa indem mit zwei Telefonen eine Kommunikation zwischen elektronischen Türschloss und Karte hergestellt wird, obwohl diese kilometerweit voneinander entfernt sind (Angreifer 1 legt Handy auf Karte, Angreifer 2 öffnet mit Handy die Tür, Karte und Tür kommunizieren übers Internet miteinander, wissen jedoch nicht davon). Gegenmaßnahme hierbei ist etwa eine “Proximity-Detection” (=”Entfernungsmessung”).