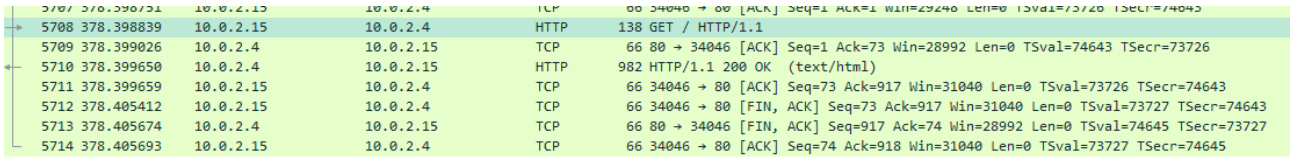
Beleg
Datenschutz und Datensicherheit

Marcus Kopp
551795

1. Aufgabe (Maschine B):
Starten Sie den ASCII-Sniffer iptraf in einem Shell-Fenster. Rufen Sie in einem anderen Fenster eine nicht verschlüsselte Webseite auf. Loggen Sie die Pakete im iptraf und schreiben Sie das Log in eine Datei.
Zur Lösung geben Sie einen Auszug aus dem Log des mit iptraf gesnifften Traffics ab.

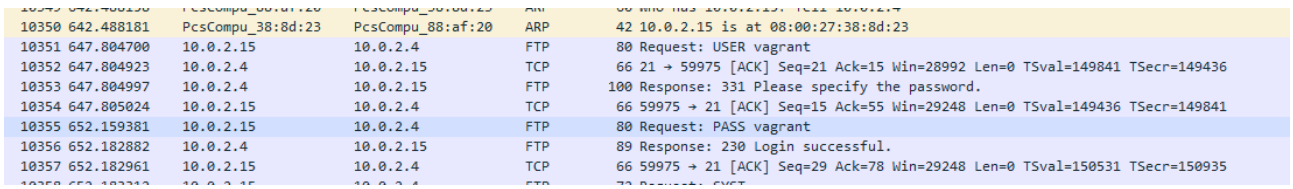
Arufruf von ping www.google.com
Tue Jul 17 10:43:29 2018; ******** IP traffic monitor started ********
Tue Jul 17 10:43:29 2018; TCP; eth0; 356 bytes; from 10.0.2.15:22 to 10.0.2.2:57756; first packet
Tue Jul 17 10:43:29 2018; TCP; eth0; 46 bytes; from 10.0.2.2:57756 to 10.0.2.15:22; first packet
Tue Jul 17 10:43:57 2018; TCP; eth0; 46 bytes; from 10.0.2.2:57788 to 10.0.2.15:22; first packet (SYN)
Tue Jul 17 10:43:57 2018; TCP; eth0; 44 bytes; from 10.0.2.15:22 to 10.0.2.2:57788; first packet (SYN)
Tue Jul 17 10:43:57 2018; UDP; eth0; 67 bytes; from 10.0.2.15:46877 to 10.0.2.3:53
Tue Jul 17 10:43:57 2018; UDP; eth0; 67 bytes; from 10.0.2.3:53 to 10.0.2.15:46877
Tue Jul 17 10:44:05 2018; UDP; eth0; 59 bytes; from 10.0.2.15:49177 to 10.0.2.3:53
Tue Jul 17 10:44:05 2018; UDP; eth0; 96 bytes; from 10.0.2.3:53 to 10.0.2.15:49177
Tue Jul 17 10:44:05 2018; ICMP; eth0; 84 bytes; from 10.0.2.15 to 216.58.211.110; echo req
Tue Jul 17 10:44:05 2018; ICMP; eth0; 84 bytes; from 216.58.211.110 to 10.0.2.15; echo rply
Tue Jul 17 10:44:05 2018; UDP; eth0; 73 bytes; from 10.0.2.15:48439 to 10.0.2.3:53

2. Aufgabe (Maschine B und A):
Starten Sie Wireshark und konfigurieren Sie es zum Mitschneiden. Rufen Sie die index.php auf Maschine B auf. Zur Lösung geben Sie ein Bildschirmfoto ab. Es sollte nur der Webseitenaufruf von A sichtbar sein.



5708	378.398839	10.0.2.15	10.0.2.4	HTTP	138 GET / HTTP/1.1
5709	378.399026	10.0.2.4	10.0.2.15	TCP	66 80 → 34046 [ACK] Seq=1 Ack=73 Win=28992 Len=0 TSval=74643 TSecr=73726
5710	378.399650	10.0.2.4	10.0.2.15	HTTP	982 HTTP/1.1 200 OK (text/html)
5711	378.399659	10.0.2.15	10.0.2.4	TCP	66 34046 → 80 [ACK] Seq=73 Ack=917 Win=31040 Len=0 TSval=73726 TSecr=74643
5712	378.405412	10.0.2.15	10.0.2.4	TCP	66 34046 → 80 [FIN, ACK] Seq=73 Ack=917 Win=31040 Len=0 TSval=73727 TSecr=74643
5713	378.405674	10.0.2.4	10.0.2.15	TCP	66 80 → 34046 [FIN, ACK] Seq=917 Ack=74 Win=28992 Len=0 TSval=74645 TSecr=73727
5714	378.405693	10.0.2.15	10.0.2.4	TCP	66 34046 → 80 [ACK] Seq=74 Ack=918 Win=31040 Len=0 TSval=73727 TSecr=74645

3. Aufgabe (Maschine B und A):
Starten Sie Wireshark und konfigurieren Sie es zum Mitschneiden. Versuchen Sie eine leere Textdatei via FTP auf A zu laden.
Zur Lösung geben Sie ein Bildschirmfoto des mitgeschnittenen Passworts ab.



10350	642.488181	PcsCompu_38:8d:23	PcsCompu_88:af:20	ARP	42 10.0.2.15 is at 08:00:27:38:8d:23
10351	647.804700	10.0.2.15	10.0.2.4	FTP	80 Request: USER vagrant
10352	647.804923	10.0.2.4	10.0.2.15	TCP	66 21 → 59975 [ACK] Seq=21 Ack=15 Win=28992 Len=0 TSval=149841 TSecr=149436
10353	647.804997	10.0.2.4	10.0.2.15	FTP	100 Response: 331 Please specify the password.
10354	647.805024	10.0.2.15	10.0.2.4	TCP	66 59975 → 21 [ACK] Seq=15 Ack=55 Win=29248 Len=0 TSval=149436 TSecr=149841
10355	652.159381	10.0.2.15	10.0.2.4	FTP	80 Request: PASS vagrant
10356	652.182882	10.0.2.4	10.0.2.15	FTP	89 Response: 230 Login successful.
10357	652.182961	10.0.2.15	10.0.2.4	TCP	66 59975 → 21 [ACK] Seq=29 Ack=78 Win=29248 Len=0 TSval=150531 TSecr=150935

4. Aufgabe (Maschine B):
Starten Sie Wireshark und konfigurieren Sie es zum Mitschneiden. Rufen Sie die Webseite https://google.de auf. Zur Lösung Beschreiben Sie den Kommunikationsablauf bis zur Auslieferung der Webseite.

a) DNS Anfrage von Maschine B (10.0.2.15) an den Heimnetz-Router (192.168.0.1)
b) Antwort des DNS Servers: Für google.de ist die IP 172.217.17.131 eingetragen
c) Aufbau zur übermittelten IP Adresse via TCP (Handshake)
d) Initialisierung der TLS Verbindung

e) TLS Server schickt Zertifikat und Server Key, Client antwortet mit Client Key
f) Verschlüsselter Handshake
g) Übertragung der Anwendungsdaten (Auslieferung der Webseite)
h) Auflösen der TCP Verbindung

5. Aufgabe (Maschine B und A):
Versuchen Sie mit nmap (auf B ausgeführt) so viele Informationen wie möglich über A herauszufinden.
Zur Lösung geben Sie eine Zusammenfassung der positiven nmap-Ergebnisse an und der nmap Befehle (inkl. Paramter) an.

```
nmap -sS -O 10.0.2.4/24
Starting Nmap 6.40 ( http://nmap.org ) at 2018-07-24 11:56 UTC
Network Distance: 1 hop
Nmap scan report for 10.0.2.4
Host is up (0.00028s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 08:00:27:88:AF:20 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see
http://nmap.org/submit/ ).
```

6. Aufgabe (Maschine A):
Installieren Sie snort. Konfigurieren Sie es so, dass es Portscanns erkennt. (Eine Vorlage zur snort.conf finden Sie im etc-Verzeichnis des Tarfiles) Es müssen mindestens drei Stellen geändert werden:
(a) Betroffene Schnittstelle
(b) Aktivieren der Portscanner-Detektoren
(c) die Reaktion bei Ereignissen, z.B. Schreiben einer Meldung in eine Logdatei
Regeldateien für Snort können nach erfolgter Registrierung unter snort.org heruntergeladen werden. Diese Regeln werden mit „tar zxf snortrules-snapshot-2820.tar.gz“ ausgepackt.
Es werden drei Ordner angelegt:
rules, preproc_rules und so_rules.
Zur Lösung geben Sie die geänderten Stellen mit den Änderungen (Endzustand) in der snort.conf an.

a) Betroffene Schnittstelle

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.2.4/32
```

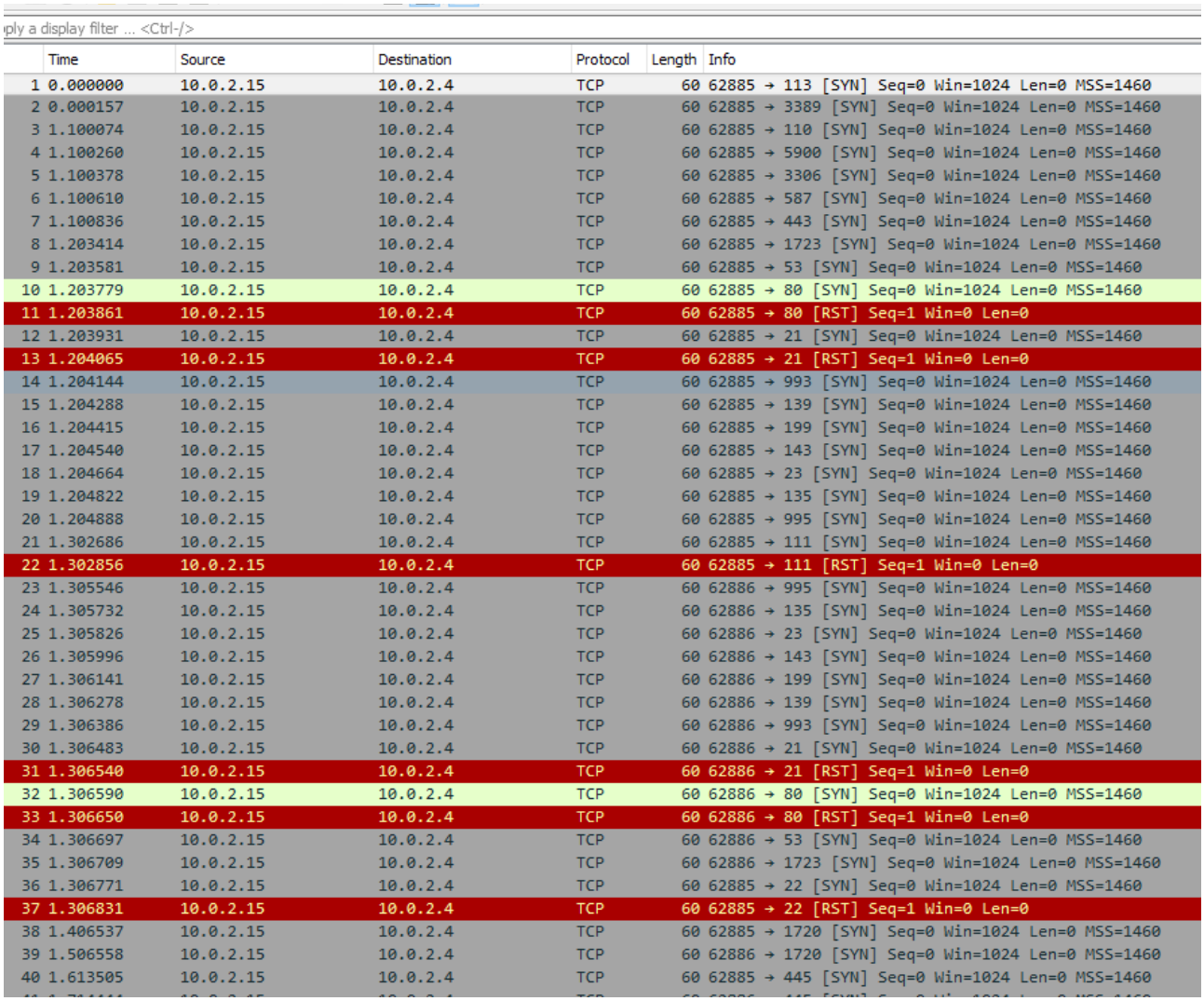
b) Aktivieren der Portscanner-Detektoren (in der local.rules)

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

c) Reaktion bei Ereignissen

```
# unified2
# Recommended for most installs
output unified2: filename snort.log, limit 128
```

7. Aufgabe (Maschine A und B):
Führen Sie Aufgabe 5 erneut durch (exkl. Abgabe der Lösung). Zeichnen Sie auf Maschine A mindestens einen Scann mit snort (Sniffer-Modus) auf (Datei). Zur Lösung geben Sie einen sinnvollen Auszug aus der Datei des mitgeschnittenen Scann ab.



ply a display filter ... <Ctrl-/>

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	10.0.2.4	TCP	60	62885 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2	0.000157	10.0.2.15	10.0.2.4	TCP	60	62885 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	1.100074	10.0.2.15	10.0.2.4	TCP	60	62885 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	1.100260	10.0.2.15	10.0.2.4	TCP	60	62885 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	1.100378	10.0.2.15	10.0.2.4	TCP	60	62885 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	1.100610	10.0.2.15	10.0.2.4	TCP	60	62885 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	1.100836	10.0.2.15	10.0.2.4	TCP	60	62885 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	1.203414	10.0.2.15	10.0.2.4	TCP	60	62885 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	1.203581	10.0.2.15	10.0.2.4	TCP	60	62885 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	1.203779	10.0.2.15	10.0.2.4	TCP	60	62885 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	1.203861	10.0.2.15	10.0.2.4	TCP	60	62885 → 80 [RST] Seq=1 Win=0 Len=0
12	1.203931	10.0.2.15	10.0.2.4	TCP	60	62885 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	1.204065	10.0.2.15	10.0.2.4	TCP	60	62885 → 21 [RST] Seq=1 Win=0 Len=0
14	1.204144	10.0.2.15	10.0.2.4	TCP	60	62885 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	1.204288	10.0.2.15	10.0.2.4	TCP	60	62885 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	1.204415	10.0.2.15	10.0.2.4	TCP	60	62885 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	1.204540	10.0.2.15	10.0.2.4	TCP	60	62885 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	1.204664	10.0.2.15	10.0.2.4	TCP	60	62885 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	1.204822	10.0.2.15	10.0.2.4	TCP	60	62885 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	1.204888	10.0.2.15	10.0.2.4	TCP	60	62885 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	1.302686	10.0.2.15	10.0.2.4	TCP	60	62885 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	1.302856	10.0.2.15	10.0.2.4	TCP	60	62885 → 111 [RST] Seq=1 Win=0 Len=0
23	1.305546	10.0.2.15	10.0.2.4	TCP	60	62886 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	1.305732	10.0.2.15	10.0.2.4	TCP	60	62886 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	1.305826	10.0.2.15	10.0.2.4	TCP	60	62886 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	1.305996	10.0.2.15	10.0.2.4	TCP	60	62886 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	1.306141	10.0.2.15	10.0.2.4	TCP	60	62886 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	1.306278	10.0.2.15	10.0.2.4	TCP	60	62886 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	1.306386	10.0.2.15	10.0.2.4	TCP	60	62886 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	1.306483	10.0.2.15	10.0.2.4	TCP	60	62886 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	1.306540	10.0.2.15	10.0.2.4	TCP	60	62886 → 21 [RST] Seq=1 Win=0 Len=0
32	1.306590	10.0.2.15	10.0.2.4	TCP	60	62886 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33	1.306650	10.0.2.15	10.0.2.4	TCP	60	62886 → 80 [RST] Seq=1 Win=0 Len=0
34	1.306697	10.0.2.15	10.0.2.4	TCP	60	62886 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	1.306709	10.0.2.15	10.0.2.4	TCP	60	62886 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	1.306771	10.0.2.15	10.0.2.4	TCP	60	62885 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
37	1.306831	10.0.2.15	10.0.2.4	TCP	60	62885 → 22 [RST] Seq=1 Win=0 Len=0
38	1.406537	10.0.2.15	10.0.2.4	TCP	60	62885 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39	1.506558	10.0.2.15	10.0.2.4	TCP	60	62886 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	1.613505	10.0.2.15	10.0.2.4	TCP	60	62885 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

8. Aufgabe:
Geben Sie an mit welchen Mitteln Sie Ihren privaten (realen oder fiktiven) Rechner/Client schützen. Erläutern welche Angriffsmöglichkeiten damit abgewehrt werden können und welche nicht abgedeckt sind.
Zur Lösung geben Sie die Darstellung des Zustands und die Erläuterung (min. 200 Worte) ab

Zustand:
4 Geräte:
- Server
- Standrechner
- Laptop
- Router

Der Router ist dermaßen konfiguriert, dass der Server per SSH von aussen erreichbar ist (ermöglicht mir den Zugriff auf private Daten von unterwegs), und gewährt den anderen Geräten des Heimnetzes Zugriff zum Internet.
Der Login auf dem Server per SSH kann neben der Eingabe von Nutzername und Passwort auch über den auf dem Laptop hinterlegten und beim Server registrierten SSH Key erfolgen, sodass eine ständige Eingabe von Nutzername und Passwort hinfällig wird. Auf dem Server läuft zudem noch die Anwendung fail2ban, welche die Logs von laufenden Anwendungen per Regex auf fehlgeschlagene Anwendungsversuche scannt. Fail2ban ist so konfiguriert, dass die entsprechend

Ips nach drei fehlgeschlagenen Anmeldungsversuchen für 12 Stunden geblockt werden. Dies dient dem Schutz vor Brute-Force- und/oder Wörterbuch-Attacken.
Auf dem Laptop läuft Ubuntu 16.04 LTS, welches wöchentlich manuell geupdated wird. Dadurch werden auch immer die neuesten Sicherheitsupdates geladen. Das System ist so konfiguriert, dass es sich nach 5 Minuten Inaktivität von selbst sperrt, und per Passworteingabe aufgeweckt werden muss. Dies kann auch manuell per Keybind erfolgen. Der Sinn dahinter ist, den Laptop vor Gelegenheitsdatendiebstahl (offener Facebookaccount in einer Kaffeepause) zu schützen. Eine grundlegende Firewall (UFW) ist eingerichtet.
Mein Standrechner läuft mit Windows 10 und bezieht automatisch die neuesten Updates. Für die Firewall wird die Windows Firewall verwendet.
Beide Rechner erlauben keinen externen SSH Zugriff (Port geschlossen), um unbefugten Einlogversuchen vorzubeugen. Neben einem Useraccount miot beschränkten Zugriffsrechten und einem separaten Adminaccount (beide mit Passwörtern gesichert) sind zudem die Festplatten mit Passphrase verschlüsselt, um meine persönlichen Daten vor physischem Diebstahl zu schützen. Gegen Keylogger oder öähnliche Attacken reichen meine Maßnahmen nicht aus, da mein Heimrechner jedoch fest Zuhause steht, und ich meinen Laptop während des Unibetriebs nie unbeaufsichtigt lasse, ergeben sich hier nicht genug Angriffsmöglichkeiten, um den Aufwand zu rechtfertigen.

9. Aufgabe:
Nennen und erläutern Sie (in Sätzen) je 4 Vor- und Nachteile einer Bring-Your-Own-Device Strategie in einem Unternehmen.

Vorteile:
- Vertrautheit: Mitarbeiter, die ihre Aufgaben auf den eigenen Geräten (und damit in einer gewohnten Arbeitsumgebung) verrichten, arbeiten effizienter und schnelletr
- Flexibilität: Mitarbeiter, die ihre eigenen Geräte für die Arbeit benutzen, sind weniger ortsgebunden und können im Home Office (oder anderswo) arbeiten.
- Geringere Anschaffungskosten: Die Firma spart Geld, da sie nicht jeder Mitarbeiter*in ein Gerät stellen muss. Zudem gehen Mitarbeiterinnen mit ihren eigenen Geräten sorgfältiger um.
- Neuere Hardware: Mitarbeiterinnen neigen dazu, neuere Hardware für sich selbst zu besorgen, als die zur Verfügung gestellten Arbeitsgeräte. BYOD macht sich dies zunutze, sodass auch die Arbeitsumgebung davon profitieren kann

Nachteile:
- Haftung: BYOD schafft Unklarheiten, wer (Firma oder Mitarbeiter*in) im Schadensfall für eine Reparatur aufkommt
- Sicherheit: Auf firmeneigenen Geräten ist es einfacher, sensible Firmendaten vor unbefugtem Zugriff zu schützen, da hier die angemessenen Sicherungsmaßnahmen sichergestellt werden können
- Kontrolle über Verwendung: Es kann nicht mehr sichergestellt werden, dass die Geräte angemessen gebraucht werden (Verwendung in unsicheren Netzwerken, Installation von unsicherer Software, etc.)
- Kontrolle über Daten: Nach Beendigung des Arbeitsvertrages kann es schwierig werden, das fachgerechte Entfernen von Firmendaten vom Gerät sicherzustellen

10. Aufgabe:
Erläutern Sie das Kerckhoffs'sche Prinzip und warum es in der Kryptografie sinnvoll angewandt werden kann.

Definition: Die Sicherheit eines Verschlüsselungsverfahrens beruht auf der Geheimhaltung des Schlüssels anstatt auf der Geheimhaltung des Verschlüsselungsalgorithmus.

Vorteile des KP:
- Geheime Algorithmen können durch Reverse Engineering rekonstruiert werden
- Fehler in einem öffentlich bekannten Algorithmus werden durch größere Menge an Reviewern schneller entdeckt
- Geheime Algorithmen können leichter um Hintertüren erweitert werden
- Schlüssel einfacher geheim zu halten als Algorithmus
- Schlüssel ist einfach auszutauschen als Algorithmus, wenn diese bekannt werden

11. Aufgabe:
Nennen Sie zwei mögliche Probleme und deren Auswirkungen, wenn ein Kryptografie-Algorithmus im Black-Box-Verfahren angewandt wird. (Black Box = Algorithmus ist nicht bekannt)

a) Schwache Zufallszahlen:
Black-Box Modell macht starke Annahmen über die Qualität von Zufallszahlen, die z.B. für die Erzeugung von Schlüsseln benötigt werden (der Praxis häufig schwierig, gute Zufälligkeit zu erzeugen)
b) Seitenkanalangriffe:
Im Black-box Modell werden kryptographische Verfahren in einer idealisierten Umgebung ausgeführt. In der Realität haben Angreifer jedoch häufig physischen Zugriff auf die Implementation, wodurch sogenannte Seitenkanalangriffe möglich werden.
c) Fehlerhafter Implementierungsprozess:
Die Sicherheitsanalyse im Black-box Modell macht keine Aussage über den eigentlichen Implementierungsprozess. Dieser ist jedoch ein wichtiger Grund für Sicherheitslücken in kryptographischen Implementationen: Der Implementierungsprozess ist nicht nur fehleranfällig, sondern kann auch leicht böswillig manipuliert werden.

12. Aufgabe:
Nutzen Sie die Viginère Chiffre und das Schlüsselwort „buchsbaeumebrauchenauchwasser“, um den folgenden Text zu verschlüsseln. Leerzeichen werden subtrahiert.

erst wenn der zu verschluesselnde text kuerzer oder genauso lang ist wie das verwendete schluesselwort ist das verfahren unknackbar

Als Lösung geben Sie die verschlüsselten Zeichen in Gruppen zu je 5 Zeichen ab.

a) Ausgangstext
erst wenn der zu verschluesselnde text kuerzer oder genauso lang ist wie das verwendete schluesselwort ist das verfahren unknackbar

b) Leerzeichen subtrahieren
erstwennderzuverschluesselndetextkuerzerodergenausolangistwiedasverwendeteschluesselwortistdasverfahrenunknackbar

c) In 5er Gruppen einteilen
erstw
ennde
rzuve

rschl
uesse
lndet
extku
erzer
oderg
enaus
olang
istwi
edasv
erwen
detes
chlue
sselw
ortis
tdasv
erfah
renun
knack
bar

d) Verschlüsseln
fluao
fnrxq
valvy
tzgul
ogzoe
dfhvu
yzacv
evtqv
pueli
lrnum
qswny
awkxc
gkstv
iliio
uengz
gulog
zoedo
siucu
avbsz
ydjby
rypbr
xnuer
xaj