Zusammenfassung IT-Security (mak)

Sicherheitsanalysen Buch

Dominic Kurmann

Christoph Schneider

Michael Koch

Aktuelle Version 1.0

|  |  |  |
| --- | --- | --- |
| **Version** | **Änderung** | **Person** |
| 1.0 | - | mk |

Inhaltsverzeichnis

Sockets, TCP/UDP (S. 37) 3

ARP-Protokoll (S. 43) 3

DHCP (S. 50) 3

ICMP & TCP (S. 64) 3

DNS (S. 78) 3

Routing (S. 85) 4

RCP (S. 93) 4

SNMP (S. 107) 4

Dienste (S. 112) 4

FTP (S. 114) 4

E-Mail (S. 135) 4

HTTP (Seite 191) 5

HTML 1 (Seite 205) 5

Active X (Seite 230) 5

HTML 2 (Seite 246) 5

Zertifikate (Seite 281) 5

HTTPS Sicherheitsanalyse 1 (Seite 321) 5

HTTPS Sicherheitsanalyse 2 (Seite 326) 5

HTTPS Sicherheitsanalyse 3 (Seite 328) 6

Authentifizierung (Seite 333) 6

TAN (Seite 335) 6

Authentifizierung (Seite 340) 6

SSH. (S.353) 6

SSH 2 (S.357) 6

Funknetze (S. 374 ff.) 6

Funknetze (S. 382) 7

Netzwerk (S. 446ff.) 7

Filtern von Datenströmen(S.450) 8

Firewalls der Arbeitsstationen (S.452) 8

Transponder (S.661) 8

## Sockets, TCP/UDP (S. 37)

Mittels RAW-Socket können Netzwerk-Pakete direkt in der Applikation empfangen werden. Daraus Resultiert die Möglichkeit einen Netzwerk-Sniffer zu betreiben. Falls unverschlüsselte Daten über das Netzwerk transportiert werden, können diese mitgeschnitten werden. Heutzutage funktioniert dies jedoch nur noch wenn ein Repeater anstatt Switch im Netzwerk verwendet wird, ein Netzwerkkabel manipuliert wird oder andere Angriffe wie ARP-Poisoning usw. kombiniert werden.

Mittels RAW-Socket können Netzwerk-Packete manipuliert werden. der Angreifer den Netzwerk-Verkehr über sich leitet, kann er Live die Pakete verändern.

Zum Beispiel kann die Absender Adresse manipuliert werden (Spoofing).

Mittels RAW-Socket können spezielle Pakete verschickt werden (SYN-Flood), die eine Serverüberlastung (DoS) zur Folge haben können. Dies funktioniert falls eine sehr grosse Anzahl von manipulierten Paketen verschickt wird.

## ARP-Protokoll (S. 43)

Manipulationen am ARP-Protokoll betreffen nur Geräte innerhalb des LAN (Broadcast Domain). ARP funktioniert auf Layer 2 und wird nicht vom Router weitergeleitet.

Alle Rechner führen einen ARP-Cache. In diesem Cache wird jeder IP eine MAC Adresse zugeordnet. Wenn wir ins Internet Verbinden, wird im ARP Cache geschaut was unser Standard Gateway für eine MAC Adresse besitzt und sendet die Pakete dahin. Der Angreifen kann ein gefälschtes Packet an das Opfer senden. Im ARP Cache des Opfers befindet sich nun bei der IP Adresse der Gateways die MAC Adresse des Angreifers. Der ganze Traffic des Opfers wird nun über den Angreifer geleitet (Man-in-the-middle).

Zudem kann die Rolle eines abgeschalteten Systems übernommen werden. Alle mit der gefälschten IP-Adresse verbundenen Rechte gehen an den Angreifer über.

## DHCP (S. 50)

Wenn ein Angreifer einen feindlichen DHCP-Server installieren kann, hat er die Möglichkeit falsche Informationen wie z.B. der Standard Gateway zu verbreiten. Daraus Resultiert wieder eine Umleitung des Internet-Verkehrs zum Angreifer.

## ICMP & TCP (S. 64)

Mittels eines Pings kann festgestellt werden ob eine Maschine online ist (kann mittels Firewall verhindert werden). Dazu kann festgestellt werden über welche Route ein Paket zum Ziel findet (Traceroute).

Mittels eines Pings können gefälschte ICMP-Störungsmeldungen an ein System gesendet werden. Dieses schliesst unter Umständen die Verbindung was einen Denial of Service zur Folge hat. Der Angreifer muss jedoch wissen wann das System eine Verbindung initiieren will.

Mittels eines Pings können gefälschte ICMP-Redirect Meldungen an ein System gesendet werden. Das System wird demnach aufgefordert eine andere Route zu wählen.

Mittels eines Pings können Informationen an externe Systeme gesendet werden. Diese werden einfach an das Packet angehängt.

Eine TCP-Verbindung wird mittels eines Three-Way-Handshakes hergestellt (SYN-SYN/ACK-ACK). Wenn der Server ein SYN erhält, werden Ressourcen für diese Verbindung allokiert. Der Server reagiert mit einem SYN/ACK. Der Angreifer sendet nun kein ACK, sondern hat nur im Sinn weitere SYN Pakete zu senden, um die Ressourcen auf dem Server aufzubrauchen (SYN-Flood).

## DNS (S. 78)

Der DNS-Server wandelt eine Internet Adresse in eine IP-Adresse um. Wenn ein Angreifer die Antwort auf eine DNS-Anfrage manipulieren kann sind wir wieder bei der Man-in-the-middle Problematik.

Das Protokoll lässt es zu, dass zusätzlich Antworten mitgeschickt werden, die gar nicht nachgefragt wurden. Bsp.: Ich frage nach der IP-Adresse für google.ch, die Antwort beinhaltet die IP-Adresse von google, sowie die IP-Adresse für windowsupdate.com.

Viele Adressen wurden mit Tippfehlern registriert, um User auf alternative Seiten zu führen (Typosquatting). Hierbei handelt es sich jedoch um eine korrekte Anwendung des DNS.

## Routing (S. 85)

Router können gefälschte Informationen über zu erreichende Netze gesendet werden, da die Quell IP/MAC-Adresse beliebig gefälscht werden kann.

Das Ziel von Angriffen auf das Routingsystem ist eine Umleitung von Informationen über kontrollierte Relaisstationen um Pakete mitzulesen oder bestimmte Verbindungen zu verhindern (DoS).

## RCP (S. 93)

Bei aktivierter Portmapper-Funktion kann ermittelt werden, welchen Dienste auf dem Server laufen.

Ein weiteres Problem ist meist die unzureichender Authentifizierung oder fehlende Verschlüsselung.

## SNMP (S. 107)

Das Simple Network Management Protocol ermöglicht die Überwachung, Fernsteuerung, Fernkonfiguration und Fehlererkennung von Netzwerkkomponenten. Die lesbaren und überschreibbaren Einstellungen sind sicherheitstechnisch von höchster Relevanz.

Diese Versionen 1 & 2 von SNMP unterstützen keine Anmeldung mit Kennwort und Benutzername. Dies hat zur Folge dass jeder User im Netzwerk mit einem passenden Programm Systeminformationen auslesen und sogar Werte verändern kann.

## Dienste (S. 112)

In heutigen Betriebssystemen laufen eine grosse Anzahl an Diensten die auf entsprechende interne oder externe Aktivitäten warten. Die meisten Dienste werden automatisch mit der Installation von Software gestartet. Dies geschieht meist unbemerkt vom Anwender.

Fehlerhafte Dienste können zur Folge haben, dass der Empfang von gefälschten Paketen die Applikation oder das Betriebssystem zum Absturz bringen.

Zudem besteht die Gefahr, dass bei einer Sicherheitslücke fremder Code auf dem System ausgeführt werden kann.

## FTP (S. 114)

Bei der Dateiübertragung mittels FTP keine Verschlüsselung verwendet. Ein Angreifer welcher den Netzwerk-Verkehr beobachtet kann das Login im Klartext sehen. Die gleiche Problematik stellt sich beim Telnet Protokoll dar.

Zugangsdaten sollten für jedes Login unterschiedlich gewählt werden. Wenn im Fall das FTP-Login bekannt wird, sollte das nicht dazu führen, das weitere Accounts kompromittiert werden können.

## E-Mail (S. 135)

Wie beim FTP oder Telnet Protokoll werden auch hier die Zugangsdaten unverschlüsselt übertragen. POP3, SMTP sowie IMAP können über SSL betrieben werden. Dies wird jedoch von den wenigsten Anwender verwendet.

Mittels E-Mail können schadhafte Dateien verschickt werden. In der Vergangenheit öffneten gewisse Software die Attachements von E-Mails automatisch.

Aufgrund der Anonymität muss jeder SMTP-Server alles entgegennehmen, was ihm zugetragen wird. Die MAIL FROM Zeile kann zudem beliebig vom Absender ausgefüllt werden.

## HTTP (Seite 191)

Domainnamen können absichtlich ähnlich geschrieben werden, um z.B. an Kreditkartendaten zu gelangen. Siehe Vortrage Facebook.

Man in the Middle Attacks können genutzt werden um an Passwörter oder Daten zu kommen. Die Daten laufen Transparent von Server – Man in the Middle – Client und umgekehrt.

Cookies können ausgelesen werden und geben Einblicke in das Surfverhalten des Users. Wird dies systematisch gemacht, entstehen noch viel genauere Daten. (Marketing, Google)

## HTML 1 (Seite 205)

Durch „Web-Bugs“ können wiederum Userverhalten aufgezeichnet werden.

Das Beispiel hier ist das Laden einer fremden Seite via IMG-Tag als 1 x 1 Pixel breites (unsichtbares Bild). Dabei wird kein Bild geladen, es werden lediglich Informationen an die Empfängerseite gesendet.

## Active X (Seite 230)

Javascript und Java sind insofern sicher, dass der User immer gefragt wird ob der eine gewisse Aktion nun wirklich zulassen will.

Im Gegensatz dazu erlaubt Active X das ausführen von fiesem Code (strukturelle Sicherheitslücken) ohne auch nur einmal nachzufragen. Glücklicherweise nur auf Windows.

## HTML 2 (Seite 246)

Der HTML Server darf keine Dateien anzeigen, die unsichtbar sein sollten. Der Server und der Skriptinterpreter müssen gegen Angriffe geprüft werden (Overflows durch überlange Eingaben). Als drittes Sicherheitsproblem wird das Skriptprogramm selbst genannte. Dumme Skripte führen zu falschen Bestellungen.

## Zertifikate (Seite 281)

Zertifikate machen das Internet grundsätzich sicherer. Es gibt aber Probleme bei der Prüfung (grosser Zeitaufwand). Geprüft werden muss:

- Ob das Zertifikat korrekt ist

- Ob das Zertifikat gültig ist

- Hat das Zertifikat eine genug hohe Sicherheitsstufe im Vergleich zum Schutz, das es gewährleisten soll? (Wurde die Identität des Antragstellers geprüft?)

- Kennt man den Inhaber und vertraut ihm? (Sitz im Ausland)

## HTTPS Sicherheitsanalyse 1 (Seite 321)

Zertifikate können mit einem Man-in-the-middle-attack unterwandert werden, und zwar folgendermassen:

- Der Angreifer kann mit einem eigenen Zertifkat die Serverrolle übernehmen

- Der Angreifer verändert das Serverprogramm so, dass keine Zertifikatprüfung stattfindet. Er übernimmt wiederum die Serverrolle

- Das Verschlüsselungsverfahren kann durch den Angreifer auf eine schwache Stufe gesetzt werden (40bit) und die Daten später entschlüsseln

## HTTPS Sicherheitsanalyse 2 (Seite 326)

HTTPS-Schlüssel sind grundsätzlich sicher. (Zwei verschiedene Hashalgorithmen in Verbindung mit 6 verschiedenen Schlüsseln) Auch Entschlüsselung von Teilen führt nicht zur kompromittierung des gesamten.

Man sollte sich viel eher die Zertifikatproblematik anschauen, als an der Verschlüsselung der Pakete zu zweifeln.

## HTTPS Sicherheitsanalyse 3 (Seite 328)

Bei schlampiger Implementierung des Servers, kann ein Angreiffer vor Aushandlung des Geheimnisses in eine Fremde Sitzung „einsteigen“. Er hätte dann Zugriff auf die Daten der fremden Sitzung.

Via Man-in-the-Middle-Attack ändert der Angreifer die Verschlüsselung beim Aufbau der Verbindung. Ist der Client schlampig programmiert fällt ihm der Unterschied seiner Verschlüsselung mit der im Zertifikat nicht auf.

## Authentifizierung (Seite 333)

Wenn es einem Angreifer gelingt die Datenleitung eines Servers temporär anzuzapfen (Putzfrauenproblem), kann er eine Passwortrücksetzung einleiten, und die geänderten Passworte „mitlauschen“. Danach hat er Zugang zum System. Das Problem ist, dass das früher oder später irgend jemandem auffallen wird. (Obacht bei Accounts die nicht mehr genutzt werden, Personen die gekündigt haben z.B.)

Eine Lösung wäre die periodische Passwortveränderung aller Accounts (Anmerkung: und Überprüfung der Datenleitungen :S)

## TAN (Seite 335)

TANs (Transaktionsnummern, einmalig verwendbare Nummer zur Durchfühurng z.B. einer Buchung)

TANs können kompromittiert werden, in dem der Angreiffer eine ähnlich lautende Domain registriert und auf Tippfehler hofft. Verirrt sich ein User auf die falsche Seite, wird entweder der Auftritt nachempfunden, oder der Traffic Durchgeschleift und die Zugangsdaten abgezweigt.

Verwendet der Nutzer nun eine TAN wird die vom Angreiffer kopiert und falsch weitergereicht. Der Server lehnt die TAN ab, der Benutzer verwendet eine weitere.

Der Angreifer besitzt nun eine gültige TAN.

## Authentifizierung (Seite 340)

???

## SSH. (S.353)

Die Authentifizierung eins Users durch einen öffentlichen Schlüssel gilt als eine der Sichersten. Jedoch muss beachtet werden, dass dies über eine „Key Card“ geschieht. Das heisst, dass die erforderliche Singnatur nicht auf dem Clientsystem erzeugt wird, sondern unabhängig von fremder Hard- und Software.

Geschieht eine Authentifizierung nur durch Name und Kennwort, können diese gerade auf unbekannten Fremdsystem leicht durch Spitzelprogramme protokolliert werden. Dieser Faktor muss besonders beachtet werden und deshalb Fremdsysteme wenn möglich gemieden.

## SSH 2 (S.357)

SHH-Tunnel können im Gegenzug aber auch eine Gefahr darstellen. Wenn sie von regulären Anwendern dazu verwendet werden, Informationen aus dem sicheren Netz unerkannt zu exportieren.

## Funknetze (S. 374 ff.)

Belauschen von Telefongesprächen ist sehr einfach geworden. Einerseits für die Behörden, andererseits auch für kriminelle. Behörden haben die Möglichkeit mit einem richterlichen Beschluss Telefongespräche anzuzapfen. Dies ist sehr einfach da alles recht zentralisiert übertragen wird. An den Übertragungsknoten gibt es die sogenannten LI-Schnittstellen(Lawful Interception). Hier kann ganz einfach ein Gespräch mitgehört werden.

Die ist für fast Jedermann machbar und viel unauffälliger ist der Einbruch mittels IMSI-Catchern. Sie können eine komplette Basisstation imitieren. Dort melden sich alle in Reichweite befindlichen Mobilgeräte an. Der Catcher schaltet dann die Verschlüsselung aus damit der Mithörer effektiv auch mithören kann. Dies ohne dass der Telefonbesitzer etwas davon mitkriegt, da die Telefon meist nicht dazu ausgelegt sind solche Vorfälle zu melden. **Ausgehende Anrufe** werden nun einfach über den Catcher durchgeleitet. Er hat also eine „Man in the middle“ Position. Da der Catcher die Verdingung weiter leiten muss. bezahlt dieser auch die Telefonkosten. Dies wird dem Abgehörten irgendwann auf Grund fehlender Kosten auffallen.

**Eingehende Gespräche** können jedoch nicht mitgelauscht werden, da der Catcher keine Anrufe entgegennehmen kann und somit eine Verschlüsselung des Gesprächs stattfindet.

## Funknetze (S. 382)

Der RC-4 Algorithmus selbst hat Schwachstellen. Er kann unter gewissen Umständen sehr leicht ermittelt werden. Somit ist die von den Internetprovidern verkaufte Sicherheit von WLAN Routern ein schlechter Scherz.

* Schwache Schüssel: Zahlenfolge die aus systematischen Gründen eine analysierbare Korrelation aufweisen
* Effektive Stärke von Schlüsseln ist nicht 64/128 bit sondern etwa 40 bzw. 102 bit. Damit ergeben sich bei einem Frontalangriff gute Chancen in das Verschlüsselungssystem einzubrechen.

Rahmenbedingungen die beim Betrieb eines WLANs eingehalten werden sollten:

* Betrieb nur verschlüsselt (128 bit)
* MAC –Adressen Filterung
* WLAN wird als Internet-Bereich konfiguriert.
* Stationen besitzen aktive Firewalls.
* Verbindungen der Mobilstationen untereinander nur mittels VPN
* Über das WLAN ist keine Internetverbindung zugänglich.

Internet und Intranet (S.437)

Bei der Installation von Servern ist besondere Sorgfalt notwendig, um keine Schlupflöcher für feindliche Angriffe zu öffnen. Speziell sind dabei die Leserechte von Server auf die Verzeichnisse zu beschränken.

Zugriffe auf Skriptprogramme müssen besonders sorgsam vergeben werden. Es kann unter anderem möglich sein, dass jemand durch ein Scriptzugriff Berechtigungen erhält die er nicht haben sollte.

Programmierung von HTML-Seiten darf keine Möglichkeit beinhalten, unerlaubt zwischen Zuständen mit verschiedenen Rechten zu wechseln.

Einen guten Weg Serverdienste zu schützen, bietet ein Proxyserver. Er kann in einer reduzierten Umgebung installiert werden und somit den direkten Zugriff auf den Server verhindern. Gefahren durch unzulässige Aufrufe und fehlerhafte Konfiguration bestehen nicht. Ausser den vorgesehenen Aufrufen nimmt der Proxy nichts entgegen.

* Er bietet auch die Möglichkeit, den Server im internen Datenverkehr ein anderes Dienstspektrum anbieten zu lassen als im externen Verkehr.

## Netzwerk (S. 446ff.)

In einem grösseren Netzwerk (Internet-, Intranet-, und Serverfirewall) haben wir ein dreistufiges Filtersystem. Der Server lässt sich nun so konfigurieren, dass er Dienste auf den Ports A, B und C anbietet jeweils jedoch mit anderen Zugriffsrechten auf die Daten. Somit kann gerade für Hochsicherheitsdaten eine zusätzliche Hürde geschaffen werden. Kommt ein Eindringling an Zugangsdaten muss er zusätzlich noch einen direkten Zugang zu einem System im internen Bereich haben.

Eine Tabelle zulässiger IP-Adressen stellt nur einen schwachen Schutz dar. Der Angreifer kann mittels einer gefälschten IP-Adresse in Datagrammen, Aktionen ausführen, die nur Netzintern möglich wäre. Er kann zwar keine Kommunikation aufbauen, da er auf Grund der gefälschten IP-Adresse keine Rückmeldung erhält. Jedoch kann er Schaden durch blockieren des Server anrichten.

Zur Abwehr wird die Paketfilterung erweitert.

* Internetfirewall weißt IP-Datagramme aus dem Internet zurück, die eine interne IP haben und von extern kommen.
* Serverfirewall weisst vom Server gesendete Datagramme zurück die nicht die IP-Adresse des Server enthalten.
* Intelligente Netzwerkkomponenten kontrollieren auf gültige Kombination MAC/IP-Adresse und geben Alarm wenn dies nicht so sein sollte.
  + Nicht ganz einfach ist die Kontrolle von Mobilegeräten die ihre IP über einen DHCP beziehen.

## Filtern von Datenströmen(S.450)

Wenig Schutz bietet ein Paketfilter wenn die Firewall bereits überwunden ist. Befindet sich ein Schadprogramm im Netz kann es zwar keine Serverports öffnen, jedoch kann es als Client agieren und von innen eine Verbindung zum feindlichen Server aufbauen. Das Hauptproblem hierbei stellen Vereinbarungen dar, die bezüglich der Portvergabe und dessen Filtrierung gemacht wurden. Werden z.B. alle Ports < 1000 als Server Ports und alle >1000 als Clientports definiert, werden alle von Internet kommenden Antworten als Clientanfragen interpretiert und ohne Filterung durchgelassen. Schadprogramme die meist hohe Serverports öffnen werden so nicht mehr erkannt.

## Firewalls der Arbeitsstationen (S.452)

Zusammenfassend können die Sicherungsmassnahmen:

* Von jedem Netzwerkbereich sind nur spezifische Server erreichbar. Nicht freigebende können weder direkt noch über Täuschung angesprochen werden.
* Server sind vor einfach DoS/DDoS-Angriffen geschützt. Die Firewall weiss SYN-Pakete ab.
* Interne IP-Adressen können nicht gefälscht werden.
* Feindliche Anwendungen können auf den Arbeitsstationen nicht als Server installiert oder angesprochen werden.

Nicht erkannt werden:

* Von aussen übermittelte schädliche Inhalte
* Durch unvollständige, jedoch zulässigen Datagrammen, können von einem internen Komplizen und einem äussern Feind versteckte Informationen ausgetauscht werden.
* Ein durch die Firewall zugelassener Client- oder Serveranwendung kann von Komplizen missbräuchlich verwendet werden.
  + Zulässige Programme werden durch Trojaner ersetzt.

## Transponder (S.661)

Transpondersysteme können als sehr sicher eingestuft werden. Geht jedoch ein Transponder verloren, besteht ein gewisses Zeitfenster für Missbrauch. Nämlich bis der Transponderverlust gemeldet ist und entsprechend gesperrt.

In Hochsicherheitsbereichen ist die Transponderidentifikation zusätzlich mit einer Code-Eingabe zu verknüpfen. Auch besteht ein gutes Potential zu Überwachung. Werden zwei Transponderschranken hintereinander postiert kann ein Eintritt bzw. ein Austritt festgestellt werden. Auf Grund der geringen Grösse eines RFID-Chips, lassen sich wichtige Objekte sehr einfach gegen Entwendung schützen.