Schutz vor Schadsoftware - Malware

1. Die Anfänge des Internets und dessen Erfolg
2. Cybercrime, Malware Typen und deren Funktion
3. Schutz vor Malware – Viren (Programme)
4. Passwörter, Anwendung und Bedeutung
5. Zusammenfassung - Fragen

1. Die Anfänge des Internets und dessen Erfolg

- **1969 4 Rechner**
- Das Internet begann im Herbst 1969 als Forschungsprojekt an der Universität in Kalifornien. Die ersten 4 Großrechner waren miteinander verbunden. Es war eine kleine Forschungsgemeinschaft mit **vertrauenswürdigen und überschaubaren Benutzern. Sicherheit und Sicherheitsfragen waren damals kein Gesichtspunkt**.
- **2018 >1 Milliarde Computer, Smartphones**
- Heute sind es etwa 3,5 Milliarden Internet Benutzer weltweit. Ca. 1 Million Webseiten sind verfügbar

Diese kommerzielle Nutzung des Internets hat auch zu einer extremen Zunahme der **Computerkriminalität – Cybercrime** geführt.

Das Internet ist ein einfaches Angriffsziel weil:

- **unzählige Eintrittsstellen**
- **zahlreiche verbundene Netzwerke**
- **viele Design- und Programmierfehler**
- **Sicherheitslücken**
- **einfacher Zugang und Nutzung von Hacking Tools**

99% der Angriffe nutzen:

- **bekannte Schwachstellen**
- **Konfigurationsfehler**
- **Mangel an Bewusstsein der Nutzer für Informationssicherheit.**

2. Cybercrime - Malware
Typen und deren Funktion

- Bei der Verarbeitung von elektronischen Informationen entstehen Risiken wenn Computer an das Internet angebunden werden. Diese kann man wie folgt zusammenfassen:
- **Verlust von Daten**
- **Missbrauch von Daten**
- **Datendiebstahl**
- **Infiltration von Malware (Viren, Würmer, Trojaner etc.)**
- **Sabotage**
- **Vertrauensverlust – Wettbewerb – Werbung**
- **Spionage**
- **Verlust, Verfälschung von Nachrichten (Fake News)**

Wer sind Cyberkriminelle

- **Insider (Mitarbeiter im eigenen Unternehmen)**
- **Script Kiddies (ohne tiefere Kenntnis, Spieltrieb. Neugier)**
- **Hacker (CCC Chaos Computer Club, Aufdeckung von Schwachstellen)**
- **Computerspezialisten (Professionelle Datendiebe, Geheimdienst Mitarbeiter)**
- **Kriminelle (Erpresser, Drogenmafia etc.)**
- **Terroristen (Kommunikation, Koordination von Anschlägen, Propaganda)**
- **Industriespione und Geheimdienste (Spähprogramme PRISM, pol. u. wirtschaftl. motiviert (Stuxnet))**

Malware Typen

- Zero Day Exploits
- Viren
- Würmer
- Trojaner
- Keylogger
- Botnetze
- Rootkits Backdoor
- Adware
- Spyware
- Scareware
- Rogueware
- Ransomware

Zero-Day-Exploits

- **Einige dieser Sicherheitslücken sind nur einer kleinen Anzahl von Hackern oder Geheimdiensten bekannt.**
- **Zero-Day-Exploits sind Schwachstellen für die es noch keine Patches gibt da es dem Hersteller noch nicht bekannt ist und die Entwickler noch keine Zeit hatten diese Lücke zu beheben.**

- **Diese Exploits werden im Internet für hohe Summen gehandelt, und auch von Regierungen erworben.**

- **Es gibt Firmen die mit solchen Exploits handeln. Derzeit bietet eine Firma 3 Millionen Dollar für ein Exploit das den Remote-Zugriff auf das Apple Betriebssystem ohne Mitwirkung des Benutzers erlaubt. Laut Auskunft der Firma wurden seit April 2018 bereits 4 Mio. Dollar für Exploits bezahlt.**

Beispiel für eine Schwachstelle politisch motiviert:
Stuxnet
Der Wurm Stuxnet wurde Ende 2007 in Umlauf gebracht aber erst 2010 entdeckt. Nutzte eine Vielzahl von Schwachstellen (Zero-Day-Exploits) in Windows Systemen und Netzwerken aus. Sucht nach Kontrollsoftware der Fa. Siemens zur Steuerung technischer Prozesse (Wasserwerke, Pipeline, Atomkraftwerke) dient. Wurde über USB.Stick eingeschleust und verändert unbemerkt Einstellungen der Steuersoftware. Führte zur Zerstörung der iranischen Zentrifugen bei der Anreicherung von Uran.

Beispiel für eine Schwachstelle aus dem nicht digitalen Leben:

Angenommen in einem Gefängnis überprüft das Sicherheitspersonal Pakete nicht wenn diese weniger als 500g wiegen. Ein Freund eines Insassen schickt ein Paket mit einem präparierten Kuchen in dem ein Mobiltelefon versteckt ist. Das Exploit (Paket unter 500g) enthält also den Schadcode Kuchen mit Mobiltelefon). Wenn das Sicherheitspersonal den Kuchen an den Insassen weitergibt also den Schadcode ausführt erhält der Insasse das Mobiltelefon.

Viren:

Viren sind Malware die sich selbständig in bestehende Programme integrieren. Verändert das Wirtsprogramm. Vervielfältigt sich lokal mithilfe des Wirtsprogramms. Führt zur Leistungsminderung des Systems (PC, Laptop Smartphone)

Würmer:

Schadprogramme die sich nach Ausführung selbständig über das Netzwerk oder Wechselmedien (USB Stick) verbreiten. Kann sich nach Weiterverbreitung selbst starten. Schnellere Ausbreitung als Viren. Schadcode hat oft verheerende Auswirkung. Beeinträchtigung der Leistung. Nachinstallation anderer Malware. Infizierter Rechner wird zum Bot.

Trojaner:

Sind Programme mit versteckter Schadfunktion die sich als nützliche Anwendung tarnen. Bei Ausführung der vermeintlich gutartigen Anwendung wird automatisch die Schadfunktion ausgeführt. Können sich als Dokumente oder Dateien tarnen. Schadfunktion erfolgt beim Öffnen des Dokuments. Beispiel: Vorgespieltes Login-Formular um Nutzernamen und Passwort auszuspähen. Anhang in email. PDF-Icon aber in Wirklichkeit document.pdf.exe ausführbar!!

Keylogger:

Miniprogramm das sämtliche Tastatureingaben des Benutzers und auch den Inhalt des Bildschirms aufzeichnet. Die Aufzeichnungen werden dann an den Angreifer gesendet. Identitätsdiebstahl, Banküberweisungen.

Botnetze:

Einfallstor sind Trojaner, Würmer. Ein Botnet ist ein Zusammenschluss verschiedener Computer (Bots). Der Angreifer kontrolliert über einen C&C Server (Command and Control Server) die Bots und schickt Handlungsanweisungen an die Bots die diese dann ausführen DoS-Angriff. Denial of Service an URL. Versand von Spam Emails, Klickbetrug, Bitcoin Mining. Einsatz von Ransomware (Erpressung durch Verschlüsselung).

Beispiel: 2013 wurden 2 deutsche Hacker verhaftet die einen Trojaner zum Minen modifiziert haben und damit Bitcoins im Wert von 950000 Dollar generiert hatten.

Rootkits Backdoor:

Rootkit ist Schadsoftware die einem Angreifer kontinuierlichen Zugriff auf ein gekapertes System ermöglicht. Installation erfolgt meist bei Einbruch in das System. Versucht seine Existenz zu verbergen. Weitere Schadprogramme werden von Benutzer und Antivirensoftware versteckt.

Adware:
Programme die zusätzlich zu ihrer eigenen Funktion Werbung einblenden. Kann sich auch in Web Browser einnisten wodurch auf jeder Internetseite Werbung eingeblendet wird .

Spyware:
Software die ohne Zustimmung des Nutzers eigene sensible Daten an Dritte versendet. Spionagesoftware Spähprogramme von Anbietern von Web Diensten, staatliche Behörden. Verfolgung des Surfverhalten des Nutzers, Informationsbeschaffung von Passwörten, Kreditkartendaten.

Scareware:
Versucht durch Vortäuschen von Fehlermeldungen, Virusinfektionen oder anderen Problemen den Nutzer zu verunsichern. Oft werden Strafzahlungen oder kostenpflichtige Reparaturen gefordert. Aufzählung von Rechtsverstößen des Nutzers im Namen der Polizei.

Rogueware:
Programm das eine vertrauenswürdige Herkunft vortäuscht. Z.B Säuberung des Computers wobei Schadsoftware eingeschleust wir oder Daten gestohlen werden. Rogue-Antivirus tarnt sich als Antivirusprogramm scannt Computer (nicht wirklich) findet Schadcode und fordert eine kostenpflichtige Reparatur.

Ransomware:
Schadprogramm das Daten verschlüsselt sodass der Benutzer keinen Zugriff mehr darauf hat. Fordert Geld zur Entschlüsselung. Infektion über Email-Anhänge und Trojaner. Schutz durch regelmäßige Sicherung.

Beispiel:
WannaCry im Mai 2017 infizierte und verschlüsselte Computer zahlreicher Firmen wie

- **Deutsche Bahn**
- **Honda**
- **O2**
- **FedEx**
- **Nissan**
- **Krankenhäuser.**

3. Schutz vor Malware

- **Wichtige und persönliche Daten regelmäßig sichern**
- **Manche Betriebssystem bieten Sicherungen in vordefinierten Zeitabständen**
- **Datensicherung auf externen Medien (USB Stick, DVD, NAS, Cloud, Band)**
- **Nach Datensicherung externe Medien trennen**
- **Regelmäßige Programm Updates und Updates des Betriebssystems**
- **Virenscanner – Antivirensoftware**
- **Firewalls**
- **Gesundes Misstrauen beim Installieren neuer Software**
- **Software, Apps nur aus sicheren Quellen installieren**
- **Email Anhänge nur öffnen wenn Absender bekannt ist und zuordenbar**
- **Ruhe bewahren bei Onlinewarnungen und Aufforderungen zu Strafzahlungen**

Updates:

Allgemein gilt:
Updates beheben Schwachstellen in Software und Betriebssystemen und beseitigen dadurch Sicherheitsrisiken. Sie sollten sobald verfügbar unbedingt installiert werden.

Hier unterscheidet man Programm Updates (also Updates von Programmen und Betriebssystemen): Viele installierten Programme zeigen beim Start bereits an dass Updates verfügbar sind und von der Webseite des Herstellers heruntergeladen werden können.

Bei Updates des Betriebssystems muss der Benutzer manchmal selbst aktiv werden. Microsoft z.B. bringt an jedem 2. Dienstag im Monat neue Updates für Windows heraus. Aufgrund der Zeitverzögerung sind diese dann am darauf folgenden Tag verfügbar und sollten unbedingt installiert werden.

Ältere Windows Versionen (z.B Windows XP) werden nicht mehr von Microsoft mit Updates versorgt. Man sollte deshalb mit diesen Betriebssystemen nicht mehr ins Internet gehen.

Für Apple Rechner dürften ähnliche Kriterien gelten

<u>Updates bei Smartphones</u>:

Bei Smartphones sieht das etwas anders aus und ist auch vom Hersteller abhängig.

Da Google der Entwickler von Android ist werden Smartphones von Google wesentlich länger mit Updates versorgt als andere Smartphone Hersteller wie Samsung, Huawai, HTC etc.).
Hier endet das Update bereits nach ca. 2 Jahren da neue Geräte auf den Markt kommen und die Hersteller wenig Interesse haben ältere Geräte zu unterstützen.

Hier bleibt dann nur noch die Möglichkeit ein Custom Rom mit der aktuellen Android Version zu installieren was allerdings viel Know How erfordert und auch schiefgehen kann.

- **Virenscanner:**

- **Virenscanner oder besser Antimalwaresoftware bieten Verfahren zur Erkennung von Malware wie Viren, Würmer, Trojaner, Spyware und anderer Schadsoftware. Manche überwachen auch Internetverbindungen und warnen vor unsicheren Internetseiten (Blacklists) und haben so also eine Firewall implementiert.**

- **Antimalwaresoftware funktioniert auf 2 unterschiedlichen Methoden**

- **Signaturen**
- **Anomalien**

- **Signaturen werden durch Analyse von Malware gewonnen und scannen mit Hilfe dieser die Dateien um mögliche Schadsoftware zu erkennen.**

- **Anomalien erfassen den gutartigen Zustand des Systems und vergleichen ihn ständig mit dem aktuellen Zustand. Bei Abweichung wird eine Warnung erzeugt. Das ermöglicht die Entdeckung unbekannter Malware. Führt aber auch zu Fehlalarmen.**

Antimalwarescanner sind nur so gut wie die Aktualität ihrer Signaturen. Gute Antimalwareprogramme aktualisieren die Signaturen mehrmals am Tag und machen mehrmals automatische Scans der wichtigsten Dateien.

Es gibt kostenlose Antimalwareprogramme. Meist von Firmen die auch kostenpflichtige Programme verkaufen. Diese kostenlosen haben teilweise eingeschränkte Funktionen, enthalten oftmals Werbung und aktualisieren die Signaturen weniger häufig.

Bei Befall von Schadsoftware werden die entsprechenden Dateien in Quarantäne überführt und somit unschädlich gemacht. Danach kann eine weitere Untersuchung durchgeführt werden.

Zeitschrift CT desinfect !!!

Software APPS Smartphones sichere Quellen:

Bei den mobilen Betriebssystemen wie Android und iOS sollten APPS nur aus den entsprechenden APP Stores wie Google Play Store und Apple's APP Store installiert werden. Die Store Betreiber überprüfen die APPS auf bösartiges Verhalten. Entwickler der APPS müssen sich beim Store anmelden . Berechtigungen der APPS überprüfen und einschränken. Das kann zu reduzierten Funktionen führen. Ausweg: Rooten
Bei Alternative APP Stores muss man die Installation aus unbekannten Quellen erlauben.

Die meiste Malware bei mobilen Betriebssystemen dient zur:

- **Erbeutung von Geld**
- **Versand von Premium SMS**
- **Durchführung von Klickbetrug**
- **Diebstahl von Anmeldedaten für Online Banking**
- **Standort Verfolgung**
- **Diebstahl privater Daten**

Schutzmaßnahmen bei Diebstahl sind:

- **Verschlüsselung aktivieren**
- **Verwendung von PIN oder Passwort b. Entsperren , Fingerabdruck, Gesichtserkennung**
- **Beim Kauf des Geräts auf aktuelles OS achten und Verfügbarkeit von Updates**
- **Bei jeder APP die angeforderten Berechtigungen prüfen im Zweifel alternative APP**

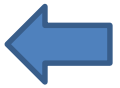
4. Passwörter und deren Bedeutung

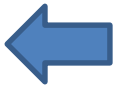
- **Um auf Dienste im Internet zuzugreifen ist meistens eine Kombination aus Benutzername und Passwort erforderlich.**
- **Diese Kombination wird bei der Registrierung bei einem Webdienst erzeugt und dient dann in Zukunft dem login auf dieser Webseite. Viele Nutzer verwenden schwache Passwörter:**
- **Aus Bequemlichkeit**
- **Weil komplexe Passwörter schwer zu merken sind**
- **Fehlendes Sicherheitsbewusstsein**

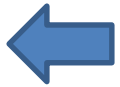
Top 10 Passwörter aus gecrackten Datenbanken mit über 150 Mio. Einträgen

Passwort	Häufigkeit	
123456	1.19%	= 1.9 Mio Benutzer
123456789	0.52%	= 832000 Benutzer
12345678	0.35%	
12345	0.19%	
password	0.15%	
111111	0.11%	
11111111	0.10%	
123123	0.09%	
1234567	0.08%	
000000	0.07%	= 112000 Benutzer

Passwort	Länge	Zeit
secret	6	<1 s
secret12	8	29 s
!sEcRe!	7	5.4 Min.
!secret2	7	1,54 h
!sEcRe!2	8	18,6 h
!sEcRe!2%9	10	19,2 Jahre







- Die Geschwindigkeit beim Brute Force Knacken von Passwörtern bei 100 Milliarden Tests pro Sekunde mit spezieller Hardware

Die sichere Speicherung von Passwörtern erfolgt meist durch Hash-Verfahren. Ein gehashtes Passwort sieht also wie folgt aus:

yH49Z%k0+ = 3cd6acc0f0fce929723014b8a9f32f91

Angriffe auf Passwörter erfolgen meist durch Erraten, Abfangen (Keylogger), Durchprobieren mittels Brute Force, Wörterbücher oder Rainbow Tables.

Sichere Passwörter sollten folgende Eigenschaften haben:

- **Länge mindestens 12 Zeichen**
- **Bestehen aus groß-klein Schreibung, Zahlen und Sonderzeichen**
- **Kein Vorkommen in Wörterbüchern (also nicht z.B. Schneeglöckchen)**
- **Keine einmal bereits benutzten Passwörter**
- **Für jeden Webanbieter ein eigenes Passwort**
- **Passwörter regelmäßig ändern, dabei nicht Teile des alten Passworts verwenden**
- **Speichern der Passwörter in Passwort Safes, USB-Stick, Cloud etc.**
- **oder manuell in einem Heft das sicher verwahrt wird. Denn was man schwarz auf weiß hat kann man getrost nach Hause tragen.**

5. Zusammenfassung
Schutz vor Schadsoftware

- **Regelmäßige Sicherung Backup von Daten und evtl. Betriebssystem auf externe Datenträger**
- **Updates für Programme und Betriebssystem installieren sobald verfügbar**
- **Benutzung von Anti-Malware Programmen (Virenschutzprogramme)**
- **Sichere Passwörter und regelmäßige Änderung der Passwörter**
- **Installation von Software nur aus sicheren Quellen**
- **Vorsicht vor Webanbietern mit dubiosen Angeboten**
- **Email Anhänge nur öffnen wenn Absender bekannt und vertrauenswürdig ist**
- **Beim Online Banking mit 2 Faktor Authentifizierung arbeiten**
- **Keine Software unbekannten Ursprungs installieren auch wenn diese noch so toll sein soll**
- **Falls es doch wider Erwarten zu einem Befall von Malware gekommen ist, Ruhe bewahren auch bei Onlinewarnungen und Aufforderungen zu Strafzahlungen und lieber um Hilfe nachfragen.**