esse

ESSE Einführung in Security – VO 09: Betriebssystemsicherheit

Florian Fankhauser, Thomas Stipsits, Christian Schanes

24W

ESSE (Establishing Security) – IT Security Research Team
Research Group for Industrial Software (INSO)
https://establishing-security.at/

Agenda

- Einschub: Die Lage der IT-Sicherheit in Deutschland 2024
- Aktuelles
- Grundlagen
- Sicherheitsziele von Betriebssystemen
- Maßnahmen zur Erhöhung der IT-Sicherheit bei Betriebssystemen
- Backdoors, Rootkits
- Literatur, Links
- Zusammenfassung

Einschub: Die Lage der IT-Sicherheit in Deutschland 2024

BSI: Die Lage der IT-Sicherheit in Deutschland 2024

- Veröffentlichung Bericht 12.11.2024
- Trends in IT-Sicherheit
- Guter Überblick über aktuelle Bedrohungen

- Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland 2024, 2024.
  `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html`

Betriebssystemsicherheit

Aktuelles zur IT-Sicherheit von Betriebssystemen

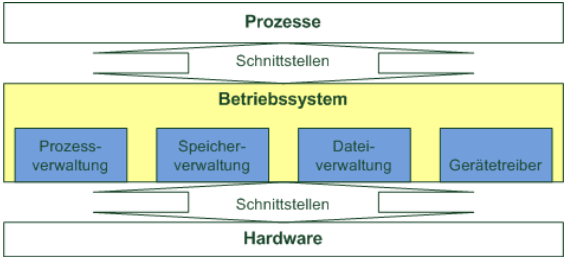
- Reboot nach Inaktivität: So funktioniert Apples neues iOS-Sicherheitsfeature
- Windows 11: Security-Updates für „das sicherste Betriebssystem der Welt“
- Fortinet stopft Sicherheitslecks in FortiOS, FortiAnalyzer und FortiClient
- Android-Patchday: Updates stopfen zwei angegriffene Sicherheitslücken
- Anonymisierendes Linux: Tails 6.9 ak tualisiert Kernkomponenten
- Apple stellt iOS 17.71, macOS 14.7.1 und macOS 13.7.1 bereit, stopft Lücken
- Sicherheitsforscher haben funktionsfähige macOS-Malware entdeckt
- Angreifer können PCs mit Virenschutz von Bitdefender und Trend Micro attackieren

Nicht mehr ganz so Aktuelles zur IT-Sicherheit von Betriebssystemen

- Android: Pixel-Handys ließen sich mit einfachem SIM-Trick entsperren
- Patchday: Schadcode über Bluetooth auf Android-Geräte schieben
- Sicherheitslücke: Codeschmuggel mit Ping in FreeBSD
- Angreifer könnten Secure Boot auf bestimmten Acer-Notebooks deaktivieren
- Root-Rechte durch Linux-Lücke
- Android-Apps können Sperrbildschirm beliebig abschalten
- Auch der Sperrbildschirm von iOS 7 hat ein Leck
- Mac-OS-X-Finder mit Pfeiltasten ausgetrickst

Aufgaben eines Betriebssystems

„Ein Betriebssystem umfasst die Programme eines digitalen Rechensystems, die zusammen mit den Eigenschaften der Rechenanlage die Grundlage der möglichen Betriebsarten des digitalen Rechensystems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen.“ (DIN 44300)



(Vergleiche Schiffmann, Wolfram: Technische Informatik 3, 2011)

Mögliche Klassifikationen und Beispiele für Betriebssysteme

- Multiuser, Singleuser
- Singletasking, Multitasking
- Desktop, Mobile
- Real-Time, Embedded
- Microsoft Windows (z.B. PC, IoT)
- Linux (z.B. Debian GNU/Linux, Grml, Qubes OS, Tails, Ubuntu, CentOS, Arch...)
- Apple macOS
- Android, iOS, watchOS,...
- BSD-Varianten (z.B. OpenBSD, FreeBSD,...)
- Raspberry Pi OS
- CISCO IOS, NX-OS
- Haiku, z/OS, Oracle Solaris, Zephyr,...

Sicherheitsziele von Betriebssystemen

- Übliche Sicherheitsziele wie
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

- → Was bedeutet das für Betriebssysteme?
- → Wie würden Sie Betriebssysteme angreifen?

Beispiele für Maßnahmen zur Erhöhung der IT-Sicherheit bei Betriebssystemen

- Berechtigungssysteme
- Firewalls
- Speicherverwaltung, z.B.
  - Address Space Layout Randomization (ASLR)
  - Non Executable Stack
- Verschlüsselung von Filesystemen
- Jails/Sandboxes (z.B. chroot), Virtualisierung
- Härtung von Systemen

Minimierung der Anzahl von Angriffsvektoren/der *Attack Surface*

- Grundgedanken für die Härtung eines Systems
  - Ein nicht installiertes Service kann nicht angegriffen werden.
  - Ein nicht vorhandenes Tool kann nicht für einen Angriff verwendet werden.
  - Ein nicht vorhandenes Recht kann nicht missbraucht werden.
- Ausgewählte Methoden der Minimierung der Anzahl von Angriffsvektoren
  - Ausschließlich Services installieren, die erforderlich sind
  - Ausschließlich Tools installieren, die erforderlich sind
  - Nur Benutzer:innen anlegen, die erforderlich sind
  - Rechte restriktiv vergeben (Benutzer:innen, Files,...$\rightarrow$ Concept of Least Privilege)

Härtung von Systemen

- „‚Härten‘ (engl. Hardening) bedeutet in der IT-Sicherheit die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind.“ (BSI: Leitfaden IT-Sicherheit, 2012)
- Ziel: Verringerung der Möglichkeiten für Angriffe
- Hardening ist prinzipiell auf allen (konfigurierbaren) Systemen möglich, unabhängig vom Betriebssystem
- Hardening ist eine zusätzliche Maßnahme, *kein* Ersatz für andere Sicherheitsmaßnahmen (wie z.B. Security Patches etc.)

Offene TCP-Ports in einer Debian Standardinstallation mit Serverdiensten

```
$ nmap [...]

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-30 06:12 CEST
Interesting ports on 192.168.1.38:
Not shown: 990 closed ports
PORT     STATE SERVICE     VERSION
53/tcp   open  domain      ISC BIND 9.5.1-P3
80/tcp   open  http        Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenny8 with Suhosin-Patch mod\_python/3.3.1
|\_Python/2.5.2 mod\_perl/2.0.4 Perl/v5.10.0)
|\_ html-title: Site doesn't have a title (text/html).
110/tcp  open  pop3        Qpopper pop3d 4.0.9
|\_ pop3-capabilities: USER EXPIRE(NEVER) UIDL X-MANGLE APOP TOP AUTH-RESP-CODE RESP-CODES IMPLEMENTATION
    (Qpopper-version-4 0 9) X-LOCALTIME(Fri 30 Apr 2010 08 14 42 0200) LOGIN-DELAY(0) X-MACRO
111/tcp  open  rpcbind
|  rpcinfo:
|  100000  2        111/udp  rpcbind
|  100003  2,3,4   2049/udp  nfs
[...]
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
143/tcp  open  imap?
|\_ imap-capabilities: LOGIN-REFERRALS THREAD=ORDEREDSUBJECT ESEARCH UNSELECT SCAN LOGINDISABLED MAILBOX-REFERRALS
    WITHIN CHILDREN BINARY IMAP4REV1 THREAD=REFERENCES STARTTLS UIDPLUS SASL-IR SORT I18NLEVEL=1 LITERAL+ IDLE
    NAMESPACE MULTIAPPEND
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
901/tcp  open  http        Samba SWAT administration server
|\_ html-title: 401 Authorization Required
|  http-auth: HTTP Service requires authentication
[...]
```

Offene TCP-Ports in einer OpenBSD Standardinstallation

```
$ nmap [...]

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-30 06:29 CEST
Interesting ports on 192.168.1.39:
Not shown: 987 closed ports
PORT     STATE    SERVICE VERSION
13/tcp   open     daytime
22/tcp   open     ssh     OpenSSH 5.3 (protocol 2.0)
|  ssh-hostkey: 1024 e9:01:93:36:3e:ca:fc:aa:fd:e7:f2:a3:c9:87:38:88 (DSA)
|\_ 2048 f5:aa:ce:f5:f7:2a:a0:7a:63:63:37:17:08:ac:ad:47 (RSA)
37/tcp   open     time?
113/tcp  open     ident
6000/tcp filtered X11
6001/tcp filtered X11:1
6002/tcp filtered X11:2
6003/tcp filtered X11:3
6004/tcp filtered X11:4
6005/tcp filtered X11:5
6006/tcp filtered X11:6
6007/tcp filtered X11:7
6009/tcp filtered X11:9
```

Offene TCP Ports Windows 10 Client Standardinstallation

OS-Version: 10.0.17763 Windows 10 Home (Redstone5 – Nov 2018)

Offener Port	Adresse	Prozess	Komponente	Verwendungszweck
135	0.0.0.0	svchost.exe	RPC Endpoint Mapper (epmap)	Abfrage von RPC-Endpoints
139	192.168.42.XXX	System	NetBIOS Session Service (netbios-ssn)	Session Management für NetBIOS Übertragungen/ Verbindungen
445	0.0.0.0	System	SMB (microsoft-ds)	Netzwerkdateisystem
5040	0.0.0.0	svchost.exe	CDPSvc Dienst	Geräte-Discovery (Bluetooth)
49664	0.0.0.0	wininit.exe	Windows Init Prozess	Undokumentiert
49665	0.0.0.0	svchost.exe	EventLog	Undokumentiert/ Systemdienst
49666	0.0.0.0	svchost.exe	Schedule	Undokumentiert/ Systemdienst
49667	0.0.0.0	spoolsv.exe	Spooler	Kommunikation mit Netzwerkgeräten zu Druckaufgaben
49668	0.0.0.0	services.exe	Services Control Manager	Administration von Services
49679	0.0.0.0	lsass.exe	Local Security Authority Subsystem	Login per AD Controller etc.

Offene UDP Ports Windows 10 Client Standardinstallation

OS-Version: 10.0.17763 Windows 10 Home (Redstone5 – Nov 2018)

Offener Port	Adresse	Prozess	Komponente	Verwendungszweck
137	192.168.42.XXX	System	NetBIOS Name Service (netbios-ssn)	NetBIOS Namensauflösung
138	192.168.42.XXX	System	NetBIOS Datagram Service (netbios-dgm)	Übertragung von NetBIOS Datenpaketen
5050	0.0.0.0	svchost.exe	CDPSvc Dienst	Geräte-Discovery (Bluetooth)
5353	0.0.0.0	svchost.exe	DNSCache	Multicast UDP DNS Message Port
5355	0.0.0.0	svchost.exe	Link Local Multicast Name Resolution (llmnr)	Namensauflösung für Hosts im selben lokalen Netzwerk
49693	127.0.0.1	svchost.exe	iphlpsvc	IP-Hilfsdienst zur Unterstützung von IPv6 Verbindungen über IPv4
58236	0.0.0.0	svchost.exe	Skype	Undokumentiert/ Systemdienst

Härten – in einer idealen Welt

- Erstellung eines Minimal-Systems
  - Auswahl sicherer Hardware
  - Service(s)
  - (Remote) Admin Utilities
  - Support Libraries
  - Betriebssystem
  - System Monitoring
- Eingeschränkte, sichere Konfiguration
- Beispiel für ein Minimalsystem und gutes Know-How
  - Linux From Scratch (LFS)

Härten – in der realen Welt

- ...immer wieder schwierig oder nicht im Fokus

- Gründe dafür sind beispielsweise
  - Fehlendes Know-How
  - Budget
  - Zeit
  - 3rd Party Software
  - Proprietäre Systeme

Härten bestehender Systeme – Umsetzung in der realen Welt

- Erforderliche Funktionen festlegen
- System installieren, updaten (nicht immer eine Option)
- Nicht erforderliche Software entfernen
- Falls nicht löschbar: nicht erforderliche Dienste deaktivieren
- Zugriffsrechte strenger setzen
- Konfigurationen überprüfen
- Default Passwörter/Geheimnisse ändern
- Weitere Maßnahmen abhängig vom System
- Anleitungen beispielsweise über CIS Benchmarks

Linux: Paketverwaltung

- Einfache (De)Installation von Softwarepaketen des Distributors
- viele Varianten (APT, RPM, Portage, iPKG)
- Paketverwaltung verwaltet Abhängigkeiten, nicht immer perfekt (z.B. bind erfordert dbus in CentOS)
- Beispiel CentOS System
  - „Minimale Installation“ → ca. 400 Pakete
  - `rpm -qa # Liste der installierten Pakete`
  - `yum remove make alsa-lib cpp ... patch wget zip`
  - Durch manuelle Entfernung von nicht erforderlichen Paketen ca. 200 Pakete incl. gewünschtes Service
  - Manche Services lassen sich nicht entfernen z.B. sendmail → Start als Service verhindern oder gegen „sicherere“ Programme tauschen

Einschränkungen von Berechtigungen unter Unix/Linux

- Berechtigungen (ls, chmod, chown, chgrp)
  - User, Group, Others
  - Weitere Modelle, unterschiedlich weit verbreitet
    - erweiterte Berechtigungen (lsattr, chattr)
    - ACL granulare Berechtigungen
    - SELinux/AppArmor
- Chroot/Jailroot, Linux Container, Docker
- suid/sgid
- Alle Benutzer:innen sind diesen Sicherheitskonzepten unterworfen, i.A. Ausnahme root

Berechtigungen

- Zugang zu IT-System
- Filesystem
- Memory
- → siehe auch VO zu Authentifizierung

Berechtigungen – Principle of Least Privilege

- Principle of Least Privilege: The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task. (M. Bishop: Computer Security: Art and Science)
- Daraus folgt mindestens
  - Nicht-privilegierte User-Accounts
  - Privilegierte(r) Administrations-Account(s), z.B. `root` in Linux oder `Administrator` in Windows
- Für unterschiedliche Aktionen sind besondere Rechte erforderlich, z.B. Installation von Programmen oder Änderung von Passwörtern
  - z.B. `sudo` oder `run0` in Linux
  - z.B. `Runas` und `UAC` in Windows

Beispiele für Berechtigungen von root

- Dateien/Ordner lesen
- Änderung von Zugriffsberechtigungen
- Wechsel der UID
- Prozesssteuerung
- Verändern von Systemparametern (Limits f. Prozesse, Filesysteme,...)
- User-Management
- System-Management (Shutdown, Reboot,...)
- Aktivierung Promiscous Mode v. Netzwerk Interfaces
- Filesysteme (un)mounten
- chroot

suid

- Viele Systemprogramme nutzen das suid-Bit
- Theoretisch kein Sicherheitsproblem
- Praktisch jedoch immer wieder fehlerhaft implementiert (z.B. Buffer Overflows)
- suid wird oft verwendet, obwohl nicht erforderlich
- Suchen von suid Programmen (als `root`!): `find / -perm -4000 -print`

chroot

- change root: / wird geändert
- Z.B. `/srv/www` → /
- Verwendung für Testumgebung
- Erhöhung der Sicherheit
- Richtige Anwendung beachten – Benutzer root
- Minimierung der Tools in einer Jail-Umgebung

Bibliotheken und chroot

- Bei dynamisch gelinkten Applikationen müssen die Bibliotheken alle aus dem Jail erreichbar sein, d.h. in der neuen durch `chroot` erzeugten Umgebung
- Statisch gelinkte Applikationen funktionieren ohne weitere Bibliotheken

- Beispiel:

```
$ ldd /usr/bin/whoami
    linux-gate.so.1 =>  (0xffffe000)
    libc.so.6 => /lib/tls/i686/cmov/libc.so.6 (0xb7dc7000)
    /lib/ld-linux.so.2 (0xb7f08000)
```

Linux-Firewall

- Backend `nftables` oder `iptables` (veraltet)
- Frontends: Commandline, GUIs
- Überwacht und filtert gesamten Datenverkehr über TCP/IP
- Einfacher Packet-Filter oder Stateful Inspection
- Hohe Flexibilität

Remote-Zugriff auf Linux

- SSH als Standard
  - Deaktiviertes X-Forwarding
  - Aktiviertes X-Forwarding
  - Verwendung von Programmen wie screen/tmux/...
- Weitere Tools wie Remote Desktop/VNC usw. ebenfalls möglich

Grundlegende Strategie zur Sicherung von Windows

- Das Starten von Programmen/Services sollte standardmäßig verboten und nur für zugelassene Programme erlaubt sein
- Ausgehender und eingehender Netzwerkverkehr sollte grundsätzlich verboten und nur für festgelegte Ausnahmen erlaubt werden
- Die automatische Nutzung von administrativen Rechten für administrativen Konten sollte deaktiviert sein
- Weitere unterstützende Maßnahmen:
  - Durchführen von (kontrollierten) Windows Updates
  - Isolierung von Software (AppContainer)
  - Einsatz der Windows Defender Advanced Threat Protection (ATP)
  - ...

Windows Firewall

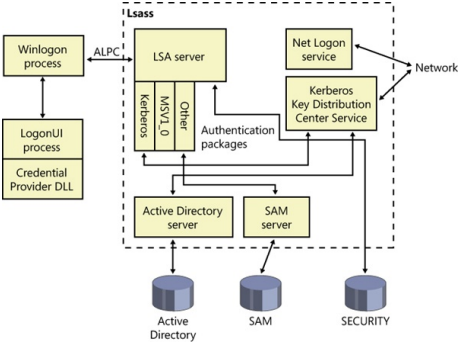
- Überwacht und filtert gesamten Datenverkehr über TCP/IP
- Ist eine Stateful Inspection Firewall
  - Zuordnung der Pakete zu aktiver Session
  - Für alle Verbindungen, welche der PC nach außen initiiert, ist eine Rückverbindung nach innen zulässig
- Erwünschter eingehender Datenverkehr muss ausdrücklich zugelassen werden
  - Ausnahmeliste mittels Portnummer, Anwendungsname oder Dienstname

Windows Zugriffssteuerung

- **Windows Rechte**
  - Benutzerkontenverwaltung & Login Prozess
  - Übersicht über NTFS-, Konten- & Benutzerrechte
  - Einschränkung des Zugriffs auf Dateien & Folder, festgelegte OS-Operationen & Anmeldearten
  - Organisation von Rechten über Gruppen
- **Windows Access Tokens vs Kerberos Tickets**
  - Identifikationsmerkmale für Benutzer/Maschinen
  - Rechteweitergabe an Prozesse und Threats
- **UAC**
  - Striktere Trennung von Administrativen und Nicht-Administrativen Vorgängen
  - Im Sinne des „Principle of Least Privilege“

Windows Login Prozess

- Credentials werden bei Login abgefragt und von Credentials Provider DLLs gehasht zu LSASS weitergegeben
- LSASS prüft Kontorechte, holt Credential-Hash von SAM und vergleicht Hashes



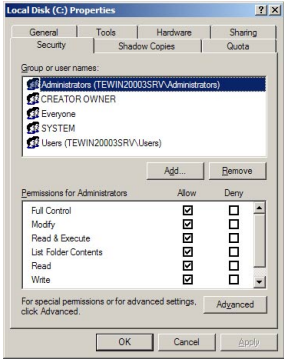
(Vergleiche https://www.microsoftpressstore.com/articles/article.aspx?p=2228450&seqNum=8)

Benutzer:innenverwaltung in Windows

- Verwaltung von Konto/Nutzerrechte, Kennwortrichtlinien, Systemüberwachung, Authentifizierung, …
- **Lokale Nutzerverwaltung**
  - Local Security Authority Subsystem Service (LSASS) verwaltet lokale Systemsicherheitsrichtlinie
  - Security Accounts Manager (SAM) verwaltet lokale NutzerDB
  - 'Administrator' (SID S-1-5-21*-500) ist der erste lokale Benutzer am System
- **Verzeichnis-basierte Nutzerverwaltung – Active Directory**
  - Nutzer, Gruppen, Computer in der Windows Domäne (Netzwerk-Domäne)
  - Zugriffssteuerung von Nutzer und Gruppen auf lokale und Domänen-Ressourcen

Windows Rechte – NTFS-Rechte

- **NTFS-Rechte**
  - Bilden Zugriffsberechtigungen auf Dateien und Folder ab
  - Werden direkt durch NTFS-Filesystem verwaltet
  - Sowohl Zugriffsrechte, als auch Share-Rechte vorhanden
  - Privilegien können über die „Datei/Ordner Eigenschaften“ Dialogbox eingesehen werden



(Vergleiche http://ntfs.com/ntfs-permissions-setting.htm)

Windows Rechte – Kontorechte

- Können mittels *C:\WINDOWS\system32\secpol.msc* konfiguriert/eingesehen werden
- Trennung in **Kontorechte** und **Privilegien**
- **Kontorechte**
  - Benutzer:innen und Gruppen erhalten innerhalb der Computerumgebung Anmelderechte
  - z.B. Lokal anmelden verweigern/zulassen, Anmelden über Remotedesktopdienste verweigern/zulassen
  - Werden durch die Local Security Authority Subsystem Service (LSASS) von der „local policy database“ abgefragt und geprüft
  - Werden im Gegensatz zu Privilegien nur Account zugewiesen und nicht durch Tokens weitergegeben

Windows Rechte – Benutzerrechte (Privilegien)

- Erlaubt es ausgewählten Gruppen/Nutzern festgelegte Operationen am System durchzuführen
- Werden durch Windows Tokens vom User an Prozesse weitergegeben
- z.B. SeShutdownPrivilege = Recht zum Herunterfahren des Systems
- Privilegien können mit *whoami /priv* angesehen werden (Nur Rechte des Nutzers, nicht seiner Gruppen)
- Teilw. kritische Privilegien – z.B: SeImpersonatePrivilege, SeSecurityPrivilege
- Müssen für erfolgreiche Prüfung vorhanden und aktiviert sein
- Werden oft durch Userinteraktion aktiviert
- Verhindert ungewollte Ausführung von privilegierten Operationen durch Prozesse

Administrative und nicht-administrative Gruppen

- Vereinfacht Konfiguration indem Privilegien über Gruppen an mehrere Benutzerkonten weitergegeben werden
- Gruppen können durch Administrator erstellt und konfiguriert werden
- Einige Gruppen sind standardmäßig vorgegeben, z.B.:

Administratoren	Vollzugriff, Zuweisung von Berechtigungen
Benutzer	Standard User-Account Gruppe
Gäste	temporäres Profil, Profile dieser Gruppe werden bei Logout gelöscht
Hauptbenutzer (Power Users)	Benutzer erstellen, lokale Gruppen,...

Windows Access Token

- Nach erfolgreicher lokaler Anmeldung erstellt LSASS ein Windows-Zugriffstoken
- Bei Login auf einen Administrator Account erstellt LSASS sowohl ein Admin-, als auch ein User-Token
- Art des Tokens je nach Sicherheitskontext unterschiedlich
- Jeder vom System erzeugte Prozess erhält eine Kopie
- Informationen aus dem Token werden benutzt, um Zugriffsrechte des Prozesses auf das jeweilige Zielobjekt zu ermitteln
- Nutzung von Kerberos Tickets und des Kerberos Authentifzierungsprotokolls in der Windows Domäne
- Nach erfolgreicher Authentifizierung bei AD Controller wird Kerberos Tickets zurückgegeben
- Kerberos Ticket wird anschließend zum Nachweis der Identität verwendet

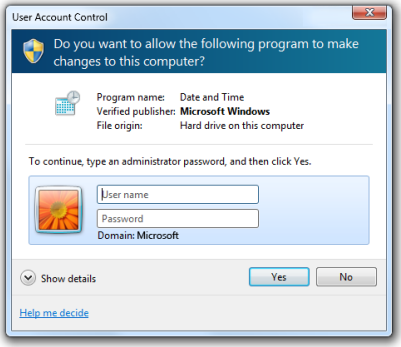
Mandatory Integrity Control (MIC)

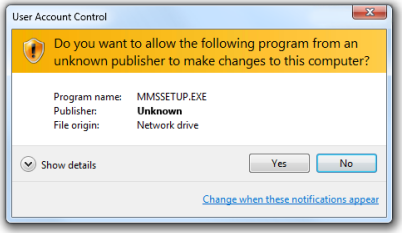
- Separierung von Prozessen hinsichtlich ihrer Vertrauenswürdigkeit
- Definieren das maximale Zugriffsrecht, das ein Prozess auf ein Windows-Objekt/Daten des Parent-Prozesses ausüben darf
- Bei Zugriff auf Ressource wird der Integrity Level des Aufrufer(prozesses) geprüft
- Unterscheidung der Integrity Levels gemäß **Security Identifier** (SID) S-1-16-xxxx:
  - S-1-16-0 – Untrusted (0x0000)
  - S-1-16-4096 – Low (0x1000)
  - S-1-16-8192 – Medium (0x2000)
  - S-1-16-12288 – High (0x3000)
  - S-1-16-16384 – System (0x4000)
  - S-1-16-20480 – Protected (0x5000, derzeit defaultmäßig nicht verwendet)

UAC – die Benutzer:innen-kontensteuerung von Windows

- User Account Control, basiert auf Integrity Levels (MIC) und Access Tokens
- Prinzipiell werden nur User-Token verwendet (auch bei Admin-Accounts)
- Bei Zugriff auf Applikationen/Prozesse, welche höhere MIC Level Aufweisen muss Zugriff erweitert werden
- Bei Admin-Accounts nur Popup, bei User-Accounts Aufforderung zur Eingabe von Admin Credentials
- Nutzung von administrativen Rechten erst durch Zustimmungsabfrage
  - (Teil-)Implementierung des Prinzips des minimalen Zugriffs
  - Zusätzliche Hürde für Malware, da Zustimmung für administrative Rechte nötig
  - Jedoch kein Schutz vor Malware, die mit reduzierten Zugriffsrechten ausführbar ist

UAC – Screenshot





(Vergleiche https://docs.microsoft.com/en-us/windows/win32/uxguide/winenv-uac)

Gruppenrichtlinien

- Steuerung von (Sicherheits)einstellungen auf dem System (siehe *C:\WINDOWS\system32\rsop.msc* oder *gpresult /R*)
- Erlaubt zentralisierte Verwaltung von Einstellungen für gesamte AD-Domäne
  - Konfiguration über Gruppenrichtlinienobjekte (GPOs)
  - Regelmässige Aktualisierung der GPOs aus der Domäne
  - Lokale GPO – Gilt nur für eine Maschine
  - Globale GPO – Gilt für alle Maschinen in Domäne
- Administrative Vorlagen für eine Vielzahl an Einstellungen, z.B.
  - Richtlinie für sichere Kennwörter
  - Konfiguration der Windows Firewall
  - Zugriffe auf Wechselmedien regulieren

Logging, Auditing

- Linux
  - primär Logfiles, z.B. `/var/log/`
    - `messages`, `syslog`, `auth`, ...
  - Texteditoren, journalctl, Snort, Zeek, AIDE,...
  - Diverse System-Tools zum Auditing (`lsof`,...)
- Windows
  - Windows erzeugt Event Logs (Ereignisprotokolle)
  - Aufgetretene Ereignisse einsehbar per Event Viewer (Ereignisanzeige)
    - Anwendungsereignisse
    - Sicherheitsbezogene Ereignisse
    - Setupereignisse
    - Systemereignisse
    - Weitergeleitete Ereignisse

Backdoors, Rootkits

„You can't trust code that you did not totally create yourself. … No amount of source-level verification or scrutiny will protect you from using untrusted code."

- Ständige Problematik von Hintertüren
- Absicht ist unentdeckt und/oder illegal
  - geschützte Daten einzulesen, und/oder
  - Änderungen an geschützten Daten vorzunehmen
- Lösung Open Source?
- Rootkit
  - Start direkt zu Beginn des Systems
  - Änderung von tiefgreifenden OS-Funktionen
  - möglichst unbemerkt von BenutzerIn

Literatur und Web-Referenzen 1/3

- Herbert H. Thompson. Why security testing is hard.
  IEEE Security & Privacy Magazine, 1(4):83–86, 2003.
  ISSN 1540-7993.
  doi: 10.1109/MSECP.2003.1219078
- Bundesamt für Sicherheit in der Informationstechnik. Leitfaden zur Basis-Absicherung nach IT-Grundschutz, 2017.
  `https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/Leitfaden-Basis-Absicherung/leitfaden-basis-absicherung_node.html`
- Matt Bishop. *Computer Security: Art and Science.*
  Pearson Education, Inc, 2003.
  ISBN 0-201-44099-7

Literatur und Web-Referenzen 2/3

- Ed Skoudis und Tom Liston. *Counter Hack Reloaded. A Step-by-Step Guide to Computer Attacks and Effective Defenses.*

  Pearson Education, Inc., 2. Auflage, 2006.

  ISBN 0-13-148104-5

- LFS (Linux From Scratch) `https://www.linuxfromscratch.org/`

- Darril Gibson. *Microsoft Windows Security Essentials.*

  Sybex, 2011.

  ISBN 978-0-7356-2174-9

- Derrick Rountree. *Security for Microsoft Windows System Administrators: Introduction to Key Information Security Concepts.*

  Syngress, 2011.

  ISBN 978-1-59749-595-0

Literatur und Web-Referenzen 3/3

- Entwicklertools, technische Dokumentation und Codebeispiele `https://docs.microsoft.com`
- Gentoo. Project:Hardened, 2017.
  `https://wiki.gentoo.org/wiki/Project:Hardened`
- SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10
- Lennart Poettering, systemd v256 release: run0,
  `https://mastodon.social/@pid_eins/112353324518585654`, letzter Abruf: 11.11.2024
- der Standard, Neu aufgesetzter Windows-XP-Rechner ist bereits nach zehn Minuten mit Malware infiziert, letzter Abruf: 11.11.2024

Zusammenfassung

- Angriffe auf Betriebssysteme finden statt
- Unterschiedliche Beispiele für Betriebssysteme
- Sicherheitsziele von Betriebssystemen
- Maßnahmen zur Erhöhung der IT-Sicherheit bei Betriebssystemen
  - Linux
  - Windows
- Härtung von Systemen
- Backdoors, Rootkits

Vielen Dank!

https://establishing-security.at/