IT-Security von A bis Z

Helmut Schweinzer
20. Mai 2023
Linuxtag der Erlanger Linux User Group

IT-Security

- Immer komplexere IT-Welt
- Dadurch zunehmend Probleme
- Man sucht Sicherheit
  - Im Vortrag geht es nicht um
    - das sichere Bedienen von Geräten (Safety)
    - Datenschutz (Privacy)
  - sondern um
    - die Sicherheit der verarbeiteten Daten (Security)

IT-Security

- *“IT-Sicherheit schützt Informationen und alle Systeme, mit denen Informationen verarbeitet, genutzt und gespeichert werden.”*
- *IT-Sicherheit muss Schwachstellen verhindern*

  Die drei Ziele der IT-Security

  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

IT-Security Wirrwarr

Es gibt viele Methoden, Techniken, Risiken, Schlagwörter, Gefahren, Empfehlungen, Richtlinien, Checklisten, HowTos, Berichte, Blogs, “Lösungen”, Schulungen, Mythen, eigene schlechte Erfahrungen, gesundes und ungesundes Halbwissen, …

→ IT-Security von A bis Z

ABC

Kleines ABC der Cyberhygiene

- Backup
- Updates
- Awareness

Backup

Kein Backup – Kein Mitleid!

- Welche Daten sichern?
- Vor welchen Risiken schützen?
- Wohin sichern?
- Wie oft sichern?
- Wie sichern?

Backup

Welche Daten sichern?

- leicht Rekonstruierbares (ganzes Betriebssystem), damit schneller rekonstruiert werden kann
- dynamische Daten (Bearbeitungsstand einfrieren)
- Archiv (Fotos)
- einmaliges (verschmerzbares)
- einmaliges (unersetzliches, “Kronjuwelen”)

Backup

Vor welchen Risiken schützen?

- Hardware-Problem → RAID
- versehentlichem Löschen → Sicherheitskopie
- Ransomware (Verschlüsseln)
- Cloud-Provider geht Pleite …
- Feuer
- Verlust (Diebstahl, Liegenlassen, …)

Backup

Wohin sichern?

- Lokal/Online
  - anderes Verzeichnis
  - andere Partition
  - andere Platte (extern oder im selben Rechner)
  - anderes Netzwerk-Share (NAS)
  - Snapshot
  - in Cloud
- OFFLINE-Backup !!
  - externe Platte(n)
  - USB-Stick
  - anderes Gerät
  - anderer Ort (Keller, Büro, bei Freund, in Schließfach, ...)

Backup Plan

Wie oft?

- öfter, wenn
  - mehr Daten sich ändern
  - sich Daten schnell ändern
  - die Daten wichtig sind
- Oder bei sinnigen Anlässen:
  - Neues Kapitel bei Dokument fertig geschrieben
  - Nach jeder erfolgreichen Bearbeitung einer Datei
  - Nach einem Tag Arbeit
  - Vor umfangreichen SW-Installationen
  - …
- Möglichst redundant sichern
- Möglichst automatisch (sonst vergisst man es)

Backup

Wie sichern?

- welche Software (rsync, snapper, BorgBackup, ...)
- Einfache Shell-Scripts / Cron-Jobs
- welche Konfiguration
  - Full (Bandbreite), Incrementell, Anzahl der Backups, online/offline, ...
  - Verschlüsselung! (luks, VeraCrypt, gocryptfs, boxcryptor, EncFS, sshfs, ...)

- Konfiguration und vor allem Anzahl der Backups kontrollieren (→ Trojaner löschen manchmal Backups).

Und nicht vergessen: Backup testen!

Updates

Updates

- Probleme
- Status
- Todo

Updates

Probleme:

- Jede Software hat Fehler (ca. 1 pro 1000 Zeilen Sourcecode)
- > 4000 ausführbare Programme in Linux
  sudo find / -type f -executable
- Es gibt strukturelle Schwachstellen (→ Security first)
- Fehlende Funktionalität (Verschlüsselung, 2FA, ...)
- und natürlich Bugs

  ... und dazu eventuell Exploits :-(

Updates

Status:

- Manches ist bekannt
- Manches wird durch Updates behoben
- Manche Features werden nachgerüstet
- Manches wird aber auch als Zero-Day ausgenutzt :-(

  … wird dadurch hoffentlich bekannt - und hoffentlich in einem Update baldigst gefixt

Updates

Die Entwicklung geht weiter

… rasant

→ nicht auf tote Projekte setzen

→ auf “benötigte Software” beschränken

→ regelmäßig aktuelle Updates/Patches einspielen, möglichst automatisch

… bei jeder Software

- Betriebssystem - Desktop, Laptop, Tablet, Smartphone, Smart-Watch
  (aber auch VPS, VMs, Docker-Container, Dual-Boot-System, Bootsticks, …)
- Anwendung (Browser, Compiler, Mailprogramm, Videokonferenz-SW, …)
- Apps im Smartphone
- Router, NAS, Drucker, Internetradio, Telefon(-Anlage), …
- Smart-TV, Spiele-Konsole, Smart-Home, Staubsaugroboter, PV-Anlage, …
- Smart-Car, …

Awareness

- Mensch als Schwachstelle
- Vertrauen
- Phishing
- Executables
- Emails
- Für Entwickler

Awareness: Mensch

Die größte Schwachstelle ist der Mensch

- → Social engineering
- Bequemlichkeit, Unachtsamkeit, Unwissenheit, Arglosigkeit

- “Gefährdet sind doch nur die Großen.”
- “Bei mir gibt es doch nichts zu holen, ich hab doch nichts zu verbergen.”

- Natürlich ist schon ein Unterschied, ob man einen Großkonzern oder nur eine Privatperson hackt.

  … aber für Algorithmen, die Schwachstellen suchen, ist das egal.

Awareness: Vertrauen

Wem oder was vertraue ich?

... und warum?

- Wenn ich einem Betriebssystemhersteller nicht traue, dann fehlt die Vertrauensbasis.

  Traue ich Microsoft?

  wenn nicht → dann eben KEIN Microsoft! → Linux - Open Source

- Wenn ein Krimineller meine Daten verschlüsselt hat, kann ich dann darauf vertrauen, dass er sie (ohne Nachforderungen) auch wieder entschlüsselt, wenn ich Lösegeld zahle?

  Oder verwendet er meine Daten danach noch gegen mich (Drohung, die Daten zu veröffentlichen), um etwas mehr herauszuholen?

Phishing

- Meine (Zugangs-)Daten werden von mir "angefragt" und dann gegen mich verwendet.

  Phishing-Mails oder Internetseiten sehen echt aus!

- Was tun:
  - Gute Passwörter mit Passwortmanager
  - Bei jedem Dienst ein anderes Passwort
  - 2FA einsetzen, wo möglich (Backup)
  - Besondere Vorsicht bei Daten für eigene Mailbox
  - Offene WLAN-Accesspoints nur verschlüsselt verwenden (https, imaps, ...)

Awareness

Auf meinem Rechner läuft ein Programm

- mit meinen Rechten und tut etwas, was ich so nicht will.
  (auch Javascript, Browser-Plugin, Makro oder in PDF, ...)

  → daher normalerweise nicht als admin/root arbeiten

- Wie wird so ein Programm gestartet:
  - Meist über Email (ausführbare Anhänge)
  - Trojaner
    (selber installiertes Programm – mit “Nebenfunktionalität”)
  - Programme mit Bugs → Update
  - Browser Drive-By-Infection → Update
  - selten (hoffentlich) über remote ausnutzbare Lücken ohne Interaktion → Update

Awareness: Emails

Email genau anschauen:

- Von wem kommt die Mail?
  - Sparkasse Support <jd4kx2@yahoo.com>
    Klarname und Email-Adresse genau anschauen

  Kann sehr einfach gefälscht werden!
- An wen geht die Email (bin ich überhaupt adressiert?)
- An wen soll die Antwort gehen?
- Welche Links sind enthalten?
  - https://google.com zeigt nicht auf Google
  - mit Mouse-Over schauen, wohin ein Link wirklich zeigt
  - manche Links sind nicht klickbar, damit Abwehrsoftware sie nicht so leicht erkennt (da muss man halt “kooperieren”)
- Anhänge:
  - Enthält ein Anhang etwas Ausführbares? (z.B. auch PDF)

Awareness: Email Kontext

Ist die Email ”stimmig”:

- Erwarte ich eine solche Mail?
  - Sendungsverfolgung
  - Rechnung
  - Konto-Information "verifizieren"
  - Angebliche Probleme mit Mailbox/Domain/...
  - “Ihr Rechner wurde gehackt”
- Erwarte ich einen Anhang?
  - evtl. auf anderem Weg bei Absender nachfragen
- Woran kann ich Unfug eventuell erkennen?
  - Ganz wichtig
  - Ganz dringend
  - Verweis auf andere Authoritäten
  - Schlechtes Deutsch

Awareness: Email Handling

Was kann ich noch tun:

- Anhänge und Links z.B. mit Online-Tool überprüfen

  → www.virustotal.com

  - Achtung: Keine persönlichen Daten hochladen
  - nur Hashes oder URLs
- Verschiedene Email-Adressen verwenden
- eigene Mails digital signieren
- SPF und DKIM verwenden, wenn möglich

Awareness für Web-Entwickler

- Never trust User Input !!!
  - Web-Formular (POST-Daten)
  - URLs mit Parametern (GET)
  - Javascript-Checks sind nett,
    serverseitige Checks sind notwendig
  - “sanitize” parameters
  - SQL-Statements selber aufbauen
  - Keine Blacklists – sondern Whitelists
- Immer https verwenden (z.B. Letsencrypt)

Awareness: Development

- KISS – Keep it stupid simple
- Zen of Python: python -c “import this”
- Fremd-Software/-Module
  - Node.js, Docker, VM-Appliances …
    - Enthalten viele fremde Pakete (Vertrauen?)
  - Github
    - Original-Projekt verwenden
      nicht eine “verbesserte Kopie” (zumindest prüfen)
    - Pull-Requests genau anschauen
- Funktions-Tests (möglichst automatisiert)
  auch nach jedem Update von Dritt-Software

Tipps

- Backup machen
- Updates machen
- Aufmerksam durchs IT-Leben “gehen”
- Bei Unsicherheit jemanden fragen
  (z.B. auch eine Suchmaschine deiner Wahl)
- Auf dem Laufenden bleiben (Security-Advisories, Changelogs, …)
- “Security-by-Design”
- Achtet auf Vertrauenswürdigkeit

Gesunden Menschenverstand einschalten!

Tag-Cloud IT-Security

Begriffe (1/2)

ABC
Audit

Backup
Backdoor
Blacklist
Bootloader
Botnet
Brute Force
Buffer Overflow

Canary
Checksum
Chroot
Cookies
CPU Bug
Crypto Miner
CTF – Catch-The-Flag
CVE

Darknet
DDOS
Defacement
Dictionary attack
DMZ
DNS-Spoofing
Domain Squatting
DOS
Drive-By Infection

Emotet
End-Point-Security
Entropy
Escrow

Fast-Flux Domains
Fingerprint
Firewall
Forensik
Fuzzying

Google Hacks

Hash
Honey Pot
HOTP
http/https

ICMP
Identity
Incident
Integrität
Internet
IOC – Indicator of Compromise

Jail
Jail Break

Keylogger

Letsencrypt
Loopback Address 127.0.0.1
LSI

Malware
Man-in-the-Middle
MFA/2FA
MITRE's ATT&CK Framework
Monokultur

NAT

Begriffe (2/2)

OSINT
OTP

Passphrase
Pentest
PDF
PFS
Pharming
Phishing
PSK

Qubes

Race Condition
Random
Ransomware
Redundanz
Responsible Disclosure
Root
Rooten

Sandbox
Secure Boot
Shodan
Smishing
Sniffer
Social Engineering
SQL Injection
SSH
SSO
Supply Chain Attack

TAILS
TOFU
TOR
TOTP
Tracking
Trojaner
TTP

Updates

Verschlüsselung
Virus
VM
VPN

WLAN
Whitelist
WoT – Web-of-Trust
Wurm

XSS
XSRF

Yubikey

Zero-Day (0-day)
Zero Knowledge
Zero-Trust

Danke für die Aufmerksamkeit

Helmut Schweinzer
Email: hel@ki-aikido.de
PGP: 0x19851166
Fingerprint: C6D3 B58F 7E3A C251 A5C5 2F89 E377 2547 1985 1166