Sicherheit

Wie sicher sind Schulnetzwerke?

Was Lehrer und Schüler (oft) nicht wissen

KNOPPER.NET
Dipl.-Ing. Klaus Knopper

Worum geht es eigentlich beim Thema „Sicherheit“?

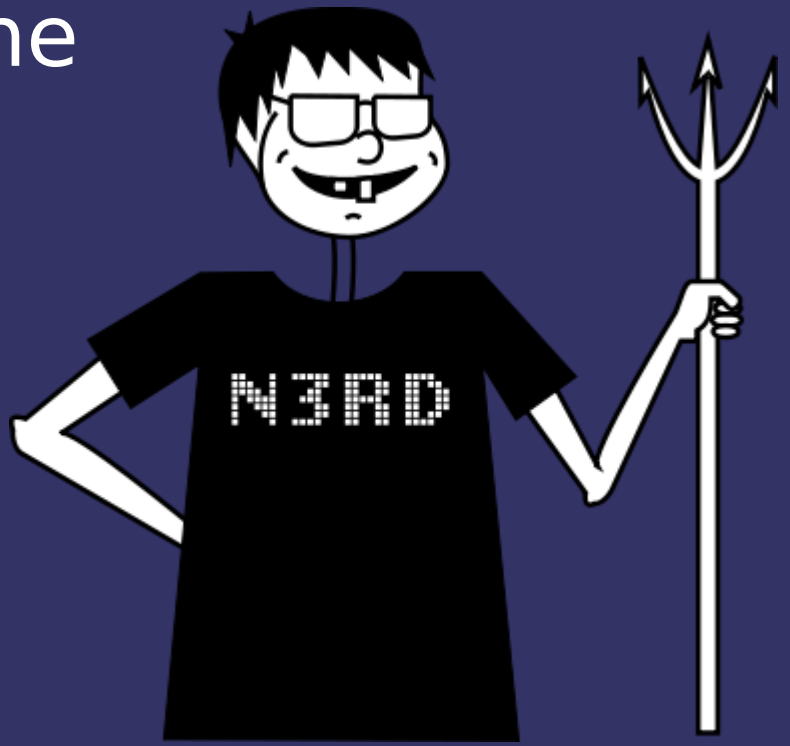
Im Wesentlichen 2 Dinge:

- Unversehrtheit der Daten (keine Manipulation des Inhalts und des Zusammenhangs)

- Vertraulichkeit (wer darf welche Daten sehen und verändern?)

Warum will jemand Daten ausspähen oder maniulieren?

- Neugier,
- Lösungen und andere Vorteile,
- Jemanden blosstellen wollen (Facebook),
- „Rache“, „Cool sein“, keine Vorstellung von den Auswirkungen.



☞ Oft haben Schüler keine *Ahnung, welche Missbrauchsgefahr durch „unwichtige Daten und Accounts“ besteht.*

Und warum will jemand meinen Computer hacken?

- Früher: „Sport, Spiel Spaß, Spannung“
  Möglichst spektakuläre Überraschungen
  Ziel: Auffallen!

  Diese Zeiten sind vorbei...

Es geht um Geld…

- Werbung für ggf. illegale Produkte und Produktfälschungen massenhaft verteilen
- Software-Nutzungslizenzen und Zugänge zu kostenpflichtigen Diensten ohne Erlaubnis der Urheber verbreiten (gegen Bezahlung)
- Illegale Inhalte verbreiten

...VIEL Geld!

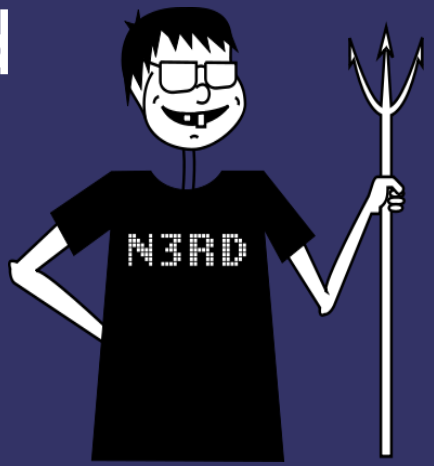
- Erpressung/Nötigung/Betrug mit falscher Identität
- Industriespionage
- Menschen-/Waffen-/Medikamenten-Handel
- Auftrags-Angriffe auf Infrastruktur zentraler Einrichtungen

Mittel zum Zweck

- Aufbau riesiger, ferngesteuerter „BOT-Netze“ aus kontrollierten Rechnern,
- „Trojaner“, um die Fernsteuerungssoftware auf möglichst vielen Rechnern zu installieren,
- Ausnutzen von Sicherheitslücken und häufigen „Fehlbedienungen“ von Systemsoftware
- UNBEMERKT bleiben!

Wie kommen Trojaner auf meinen Rechner?

Quiz: Wer arbeitet scheinbar umsonst und verschenkt großzügig und kostenlos teure kommerzielle Produkte, die man direkt herunterladen kann?



- „Warez“, „Gamez“, „Lizenzkeyz“
- Filme/Musik mit „Abspielprogramm“
- Ausnutzen von Softwarefehlern

Wer/wo sind die Hacker heute eigentlich?

- *Programmieren von Exploits*: Meist Profis mit guten System-Skills, schreiben die Crack-Programme oft sehr „Anfängerfreundlich“, denn:
- *Die eigentlichen Angreifer* haben oft gar keinen Plan von dem, was sie tun („Skript-Kiddies“),
- Beide werden für ihre Arbeit „Effizienzbasiert“ gut bezahlt, haben dementsprechend wenig Skrupel, und befinden sich meist außerhalb der juristischen Reichweite der Opfer.

Muss man gleich so schwarzsehen?

- Es gibt zwar immer weniger „stationäre“ Rechner an der Schule, aber Schadsoftware funktioniert auch, wenn man nur gelegentlich im Netz ist.
- „Bring your own Device“ verschärft die Situation, weil die Rechner nicht von Fachpersonal administriert werden.
- Die schlimmsten „Hacker“ sitzen oft im gleichen Klassenzimmer.

Und dann ist da noch die Verwaltung

- Helga interessiert sich nicht für Computer. Sie arbeitet nur damit, und achtet nicht auf merkwürdige Veränderungen.

Ist unser Netz nicht sicher?
Es gibt doch so viele Maßnahmen:

- Virenschutz!?
- Ein Firewall!?
- Ein VPN („Virtual Private Network“)!?
- Linux installieren!?

Leider nicht...

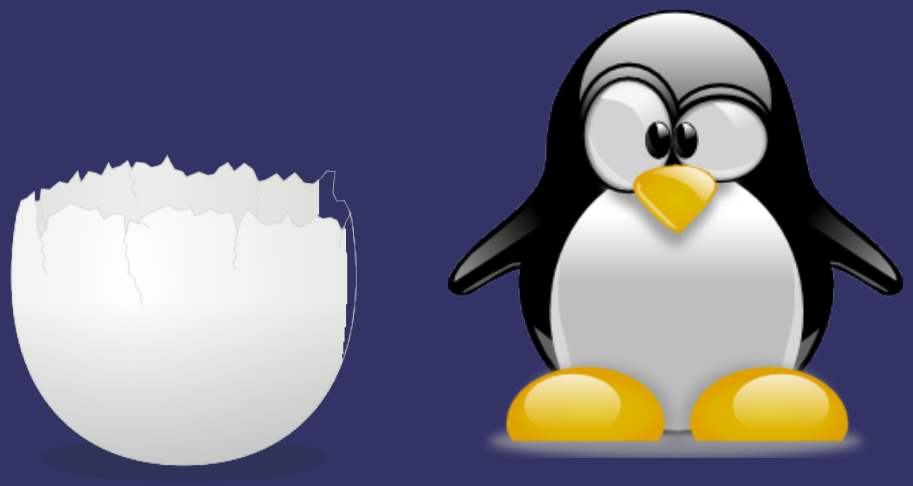
- Virenfilter filtern nur bekannte Schädlinge, keine neuen.
- Ein Firewall schützt nur bestimmte Dienste vor Zugriff von außen.
- Ein VPN verbindet Netze und erlaubt auch Zugriffe durch Schadsoftware aus dem anderen Netz.
- Linux muss auch erst sicher konfiguriert werden.

Quiz: Wie bekommen Sie als Hacker Helga dazu, Schadsoftware im E-Mail Anhang anzuklicken?

Ganz einfach: Sie schreiben dazu, dass Helga das Attachment anklicken soll.

Linux ist sicher, Open Source ist sicher… aber auch nur richtig administriert!

- „Default-Installation“: Viele nicht benötigte Netzdienste laufen „einfach so mit“, und ermöglichen bei schlecht gewählten Passwörtern Zugriff von außen.
- Sicherheitslücken können genauso bei GNU/Linux auftreten wie anderswo und müssen durch Updates behoben werden.



Statistik

- Ein frisch installierter Windows-Rechner ohne aktivierte Sicherheitsupdates „überlebt“ in stark öffentlich genutzten Netzen nur ca. 40 Sekunden, bevor er mit Schadsoftware kompromittiert ist.

- Ein frisch installierter GNU/Linux-Rechner mit schlechten Passwörtern oder völlig offen (ver-)konfigurierten Systemdiensten hält nicht wesentlich länger.

Das alles interessiert Helga aber überhaupt nicht...

- Sicherheit soll keine Einschränkung in der Arbeit bedeuten.
- Sicherheit soll am besten gar nicht auffallen, sondern im Hintergrund laufen. Am besten sollte sich überhaupt jemand anders darum kümmern...
  (Und das sehen viele Schüler genauso!)

Technik und Know-How

- Genaue Planung des Netzwerkes und der verwendeten Dienste.
- Backup DER ARBEITSDATEN mit ÜBERPRÜFUNG.
- Weiterbildung sowohl der Techniker als auch der Anwender (jawohl, auch Helga!), damit die Sicherheit leicht fällt.

Top 5 der „Ewigen Wahrheiten“

- „Meinen Rechner will sowieso niemand hacken.“
- „Wenn man nicht verrät, wie etwas funktioniert, bekommt es auch keiner heraus. Dann ist es sicher.“
- „Meine Daten sind durch ein Passwort geschützt.“
- „Verbote verbessern die Sicherheit.“
- „Die MAC-Adresse ist unveränderlich.“
- „Gelöschte Daten sind weg.“

Was man ohne viel Aufwand tun kann

- Überprüfen, was auf dem eigenen Rechner so alles läuft, was nicht laufen muss.
- Security-Plugins für den Browser, z.B. „Noscript“.
- Herkunft von Programmen und Dokumenten prüfen.
- Eigene Arbeit regelmäßig archivieren.
- Warnungen nicht ignorieren, (gerade dann) wenn man nicht weiß, was sie bedeuten.
- Verstehen, was passiert.

Netzdienste mit Anmeldung

- Die kritische Stelle, an der Hacker mit relativ wenig Aufwand Zugangsdaten abgreifen können.
- Die gleichen Zugangsdaten funktionieren meist für verschiedene Dienste (E-Mail, Infoserver, Netzlaufwerke & Cloud).
- „Identitäts-Diebstahl“: Die Verlässlichkeit und das Vertrauen in die Person geht verloren, wenn man sich nicht auch die Authentizität verlassen kann.

Beispiele von Schülern

- Manipulation von Facebook-Profilen zur Diskreditierung der Person.
- Versenden von „kranken“ E-Mails oder Posten von unsinnigen Inhalten in Foren unter falscher Identität „zum Spaß“.
- Veröffentlichen privater Unterhaltungen.
- Es fehlt das Bewusstsein, dass der Zugriff auf Information nicht lokal begrenzt ist, und Inhalte an vielen Stellen dupliziert werden.

- Marketing: Sicherheit ist ein Produkt, bei dem man gar nicht wissen will, wie es funktioniert.

Die Wahrheit

- Die Sicherung der digitalen Identität kann nur durch konsequente Nutzung sicherer Mechanismen gewährleistet werden: **Verschlüsselung** und **digitale Signatur.**

- Auch die „ausnahmsweise“ Nutzung nicht gesicherter Zugänge kann eine Ausnahme zu viel sein.

Verschlüsselung

- Zugangs- und andere Daten werden mit einem Schlüsselpaar ver- und entschlüsselt.
- Bei asymmetrischen Verfahren („Public/Secret Key“) wird ein Schlüssel zum VERschlüsseln, und ein komplementärer Schlüssel zum ENTschlüsseln verwendet. Der „geheime“ Schlüssel wird niemals übertragen.
- Bei symmetrischen Verfahren muss zuvor ein sicherer Austausch des Schlüssels stattfinden.

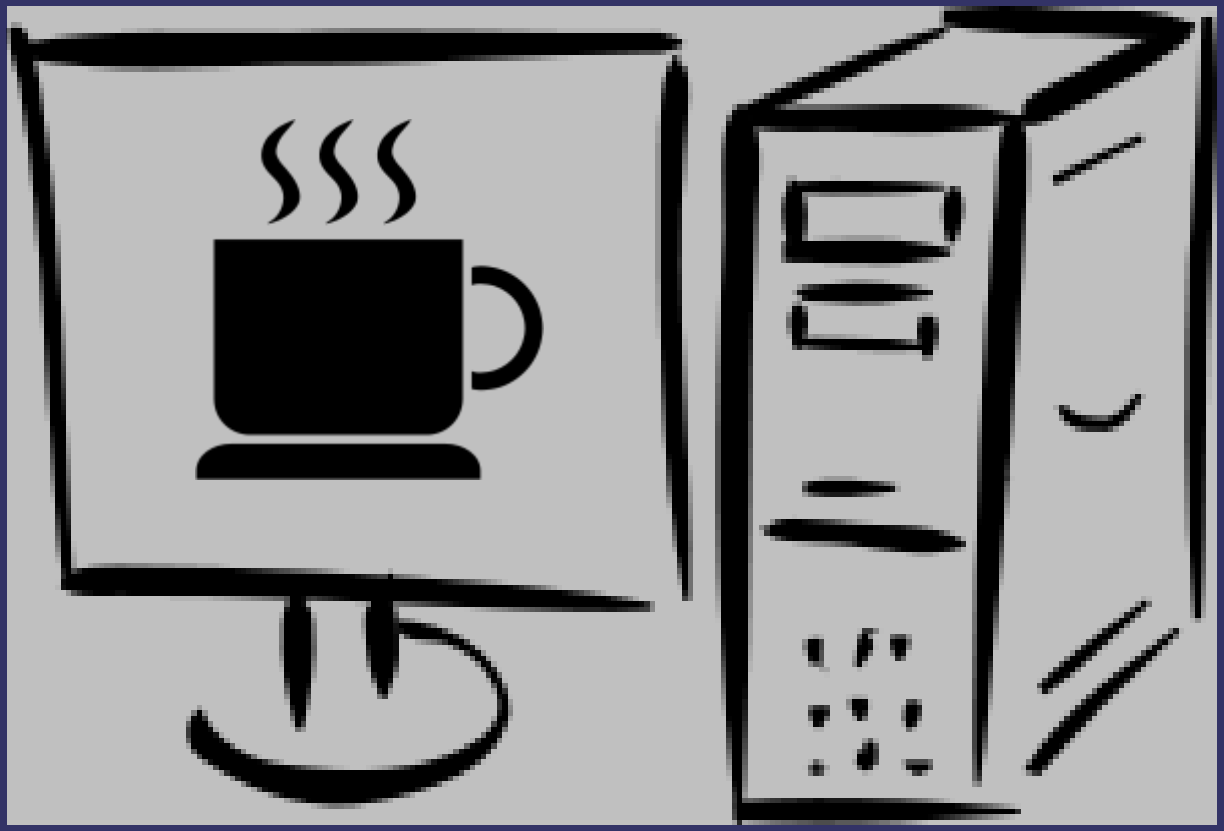
Signatur

- E-Mails oder Dokumente werden „gehasht“, die Prüfsumme wird mit dem geheimen Schlüssel des Autors unterschrieben.
- Der Empfänger kann mit dem öffentlichen Schlüssel des Autors überprüfen, das das Dokument nicht verändert wurde und vom richtigen Autor stammt.
- Die Herkunft des öffentlichen Schlüssels muss aber gesichert sein!

Wie macht man das?

- In den Medien wird zwar viel über böse Hacker berichtet, aber nicht, warum diese Erfolg hatten und wie man es verhindern kann.
- Die Mechanismen zur Verschlüsselung und Signatur sind in vielen Programmen schon eingebaut, werden aber oft nicht benutzt, weil nicht bekannt.
- Woher bekommt man ein Schlüsselpaar? (→ Nächster Vortrag)

Fragen?



security@knopper.net