Personal Firewalls – Ein Überblick

Ralf Hildebrandt
Code Blau GmbH i. Gr.
hildeb@codeblau.de

21. März 2002

Zusammenfassung

"personal firewalls": Nutzen und Gefahren, wogegen kann geschützt werden - wogegen nicht?

Sicherheit

Sicherheit ist ein dynamischer Prozess:

- Installation ist nicht genug ("shoot-yourself-in-the-foot")
- massive Fluktuationen in Funktionalität und Wissen über Exploits
- bloss weil man den Fehler nicht kennt, ist er nicht da?

Open Source

Sicherheitstechnologien müssen ausgereift und sicher sein.

Open Source Software garantiert ein Höchstmäß an Sicherheit durch die offene und herstellerunabhängige Entwicklung.

Zusätzlich ist sie extrem stabil und leistungsfähig.

Deshalb wird Open Source auch von der NSA[1] und dem deutschen BSI empfohlen.

codeblau (`http://www.codeblau.de`) setzt ausschließlich OpenSource Software ein.

[1] no such agency

Überblick

- Bedrohungspotential
- Echte Bedrohungen
- Wie funktioniert eine “personal firewall”?
- Wogegen kann eine “personal firewall” schützen?
- Wogegen kann eine “personal firewall” **nicht** schützen?
- Zusätzliche Komplexität
- “Security Desaster”
- Produktvergleich
- “Security by design”
- Fragen und Diskussion

Bedrohungspotential

Das typische Endnutzersystem. . .

- hat zuviele Dienste aktiviert. . .
  - die unsicher konfiguriert sind
  - die durch veraltete, fehlerhaft Software realisiert sind
- ist schlecht gewartet. . .
  - da Updates vernachlässigt werden
  - da das Betriebssystem inherent unsicher ist
  - da Updates die Funktionalität benötigter Applikationen unterminieren
- ist inherent unsicher
- ist dem Internet direkt ausgesetzt
- ist schlecht administriert

Echte Bedrohungen

Typische Endnutzersysteme. . .

- sind virenanfällig. . .
  - da die Firmenpolitik die zu benutzenden Programme vorschreibt
  - da die Benutzer Programme installieren dürfen
  - da die Voreinstellungen des Systems nicht restriktiv genug sind
  - da der Benutzer nicht geschult ist
- sind trojaneranfällig
  - da unprivilegierte Benutzer Programme installieren dürfen
- sind "exploitable[2]"
  - da auf dem System alte, unsichere Software eingesetzt wird
- sind "high-value Targets"
  - da auf dem System interessante Daten gespeichert sind
  - da das System als Sprungbrett für weiteren Missbrauch genutzt werden kann wie z.B.

[2] mißbrauchbar

Funktionsprinzip

Eine “personal Firewall”. . .

- verhindert ein Eindringen indem der Zugriff auf Netzwerkports – “Eingänge” in den Computer, die für bestimmte Dienste wie HTTP oder Email benutzt werden.
- filtert den Netzwerkverkehr von und zum eigenen Rechner. . .
  - anhand eigener, individueller Regeln, die vom Benutzer angepasst werden können
  - mittels einer zusätzlich zu installierenden Software
- generiert Alarmmeldungen, auf die der Benutzer reagieren kann
- Unglücklicherweise können Firewalls ganz schnell zu einem Problem werden: Indem sie verhindern, daß Sie Ihre eigenen Programme nutzen können oder sogar Programme behindern, von denen Sie gar nicht wußten, daß sie überhaupt das Internet benutzen!

Schutz?

Eine "personal firewall" bietet Schutz vor. . .

- Netzwerkbasierten Angriffen wie z.B.
  - Portscans
  - "Exploits" von Software, die Netzwerkfunktionen benutzt
  - "DoS[3]"-Attacken (denial of service) in beschränktem Ausmaß ("ping of death")
  - Zugriff auf Rechnerresourcen, die netzweit freigegeben sind:
    * Drucker
    * Dateien
    * Maildienste
    * Remote Access Dienste (Citrix Metaframe, VNC, Timbuktu)
    * installierte, simple Trojaner
    * Backdoors
    * Zombies
    * Bots
    * sonstige Dienste. . .

[3] Denial of Service

Kein Schutz?

Eine “personal firewall” bietet **keinen** Schutz vor. . .

- Angriffen von “innen” wie z.B.
  - Viren
  - Trojanern
  - Angriffe, die mittels erlaubtem Netzwerkverkehr agieren und kommunizieren, also:
    - Email
    - HTTP/HTTPS
    - sonstige, explizit erlaubte Dienste. . .
  - Angriffen aus einem “vertrauenswürdigen” Netz (Intranet)
  - Angriffen auf die Firewallsoftware selbst (!)

complexity breeds bugs

Kann man ein bereits komplexes, unsicheres System durch Hinzufügen von weiterer Software auf magische Weise sicher machen?[4]

Beispiele von "bad practices":

- Enge Verknüpfung von Browser und Betriebssystem
- Nutzung unbekannten Codes von zweifelhafter Herkunft
- nachgewiesene Schwachstellen in allen Produkten
- Warum ist die Firewall nicht schon im System integriert?

[4] Dies ist eine rhetorische Frage

Security desasters I

ISS[5] BlackIce Defender: DOS Attack (9. Februar 2002)

Product version: **All** versions on **all** platforms prior to 2.9car (2.9caq is patch for the DOS attack)

Attack type: Remote denial of service, **remote execution of code with system privilege**.

BlackICE Defender is a Windows-based personal firewall and intrusion detection system. It's designed for use on home and small office PCs as well as **enterprise deployments**.

Both scenarios are available to network-based (remote) attackers capable of sending ICMP packets (typically "pings": echo request and echo reply packets) to systems running the software. The DOS exploit requires **no specific exploit tool – common tools** such as the `ping` utility distributed with typical operating systems are sufficient to generate the required packets.

[5] Internet Security Systems is the trusted security provider for its customers, protecting digital assets and ensuring safe, uninterrupted business operations

Security desasters II

ISS[6] BlackIce 2.9 car with patch: DoS attacks with `URG` flag set are **not** logged.

If you mount a DoS attack against an Blackice Server protected box, nothing of your attack will be logged by BlackIce.

This means you cannot trust BlackIce Logs if you were attacked using the same type of attacks.

A packet crafted with `URG` flag set to `1` and all other flags set to `0` will pass undetected.

[6] Internet Security Systems is the trusted security provider for its customers, protecting digital assets and ensuring safe, uninterrupted business operations

Vergleich verschiedener Produkte

Verschiedene “personal firewalls”:

- BlackICE Defender
- Symantec[7] Personal Firewall
- Zone Labs ZoneAlarm
- Microsoft Internet Connection Firewall for Windows XP
- netfilter
- Stroud’s Winsock List

[7] Wipe Info uses hexadecimal values to wipe files. This provides more security than wiping with decimal values.” – Norton SystemWorks 2002 Professional Edition User’s Guide

“secure by design”?

Sicherheit kann einzig und allein gewährleistet werden durch. . .

- schonungslose Aufdeckung aller bekanntgewordenen Fehler
- schnelle und korrekte Behebung dieser Fehler
- Offenlegung des Quellcodes, damit:
  - man sich überzeugen kann, daß keine offensichtlichen Schwachstellen existieren
  - Fehler notfalls selber behoben werden können
  - Sicherheit nicht durch Geheimniskrämerei (“security by obscurity”) hergestellt wird

Fazit

User-Systeme sind unsicher weil:

- schlecht gewartet
- schlecht konfiguriert
- keine Updates installiert werden
- das Sicherheitsbewußtsein fehlt

Damit eine Personal Firewall überhaupt eine Chance hat, die Systemsicherheit zu erhöhen, muß sie aber:

- gut gewartet
- gut konfiguriert
- auf dem aktuellen Stand sein.

Ergo:

- Effekt = Null
- Personal-Firewall = Marketing-Gag

Was nun?

Stattdessen:

- Schulung der Mitarbeiter
- Organisatorische Massnahmen:
  - Nutzungsvereinbarung
  - User darf keine Software installieren
  - usw.

Links

- ZoneLabs Website (`http://www.zonelabs.com`):
  - ZoneAlarm
  - ZoneAlarm pro
- BlackIce Website (`http://www.blackice.com`):
- Bruce Schneier's Counterpane
- Gibson Research Corporation

Diskussion