
IT-Sicherheit

IT-Sicherheit

Teurer Schutz oder bezahlbare Sicherheit?

Uta Roßberg

Fraunhofer-Institut für
Software- und Systemtechnik ISST

Berlin, 24. Februar 2006



Motivation

»Information ist heute das wichtigste Gut
in einem Unternehmen!«

Wettbewerbsfaktoren Kundenvertrauen
 Verfügbarkeit
 Kosten

Folgerung IT-Sicherheit ist kein Selbstzweck, sondern ein
 entscheidender Wettbewerbsfaktor



IT-Sicherheit — Definitionen

Sicherheit	bedeutet grundsätzlich das »Freisein von Gefahr«
Gegenstand	Informationen, IT-Systeme und Prozesse
Anforderungen	an Verfügbarkeit, Integrität und Vertraulichkeit (IT-Sicherheitsziele)
Sicheres Zusammenwirken	von Technik, Organisation und Menschen im gesamten IT-System in der konkreten Einsatzumgebung
Datenschutz	Schutz des Einzelnen vor Beeinträchtigung in seinem Persönlichkeitsrecht durch den Umgang mit seinen personenbezogenen Daten

IT-Sicherheit ist Risikomanagement

Ziel	Sicherung der langfristigen Existenz des Unternehmens
Risiko (Wikipedia)	Kalkulierte Prognose eines möglichen Schadens
Quantifizierung	Schadenshöhe und deren Eintrittswahrscheinlichkeit
Schadenshöhe	Abhängigkeit von IT steigt <ul style="list-style-type: none">• E-Commerce, Logistik, Kommunikation, ...
Eintrittswahrscheinlichkeit	Komplexität der IT steigt <ul style="list-style-type: none">• Funktionsumfang, Schnittstellen• Vernetzung (LAN, WAN, WLAN, SAN, ISDN, GSM, VPN, VoIP, UMTS, Bluetooth, ...)

IT-Risiken müssen durch Maßnahmen begrenzt werden!

Risiken — direkte und indirekte Schäden bzw. Kosten

Fehlende Leistungserbringung	durch Nichtverfügbarkeit von IT-Systemen
Rufschädigung	Unzuverlässigkeit, Geheimnisverrat, Vertrauen
Haftpflicht	Schäden durch Missbrauch eigener IT-Systeme oder Verbreitung von Viren, Nichterbringung von Leistungen o.ä.
Rechtliche Folgen	Strafanzeigen, z.B. Verbreitung illegaler Inhalte - wie Kinderpornographie, Lizenzverstöße, Datenschutz
Finanzschäden	Höhere Kreditkosten bei schlechterem Rating durch Banken – BaselII
Wettbewerbsnachteile	schlechteres Sicherheitsrating als Konkurrenz, Kosten durch Personalbedarf

Abhängigkeit von IT

IT-Ausfälle unterbrechen Geschäftsprozesse

Gefährdungen nach BSI

Höhere Gewalt (15)

Organisatorische Mängel (101)

Menschliche Fehlhandlungen (76)

Technisches Versagen (52)

Vorsätzliche Handlungen (126)

Ausnutzung mehrerer Schwächen möglich!

Potenzierung durch Komplexität

Beispiel

Ausfall der österreichischen Gesundheitskarte



Gefährdungen

Herkunft	von Innen und Außen
Malware	»malicious software« <ul style="list-style-type: none">• Viren - Passiv verbreitetes Schadprogramm• Würmer - Aktives Ausbreiten eines Schadprogramms• Trojanische Pferde - Getarntes Schadprogramm• Hoaxes - Schaden durch Verunsicherung• Schadprogramme zum Abhören und Stören
Angriffe	Denial of service (DOS), Distributed DOS (DDOS) Abhören, Informationen sammeln, »social engineering« Eindringen - Übernahme und Missbrauch von IT-Systemen



Angriffe — Phasen

Nach Brockhaus

Annäherung
Einbruch
Kampf durch die Tiefe
Durchbruch
Erreichen des Ziels

IT-Angriff

Informationen sammeln - Scan, social engineering
Eindringen - Schwachstellen, Passwörter
Kontrolle übernehmen - Schwachstelle
Spuren verwischen - Konfiguration
Nutzung - Abhören, Manipulation, Bot-Netz

Ausnahmen

Störsender



Bedrohung durch Komplexität

Software-Komplexität ist proportional zum Quadrat der Anzahl der Zeilen im Quelltext. Bsp.: IE 220% pro Jahr, PDF

Effekte

Systeme werden nicht verstanden

- Angriffe schwierig vorhersagbar
- Gefahr von Fehlkonfigurationen
- Erreichen sicherer Zustände wird unmöglich

Ansteigen der Fehlerrate in der Software

Auch Sicherheitssoftware betroffen (Virens Scanner, Firewall)

Resultat

SANS Institute - Top 20 Internet Security Vulnerabilities
<http://www.sans.org/top20/>



Abwehrmaßnahmen

Das Versagen einzelner Elemente ist einzuplanen!

Vor dem Angriff

angepasstes Sicherheitskonzept
Securityscanner – Vulnerabilitycheck
Firewall
Contentscanner – Contentwall
Verschlüsselung
Redundanz – Server, Netzwerk

Während des Angriffs

Intrusion Detection
Notfallplan/Katastrophenplan

Nach dem Angriff

Notfallplan
Forensic Computing - Beweissicherung



System »härten«

Angriff »erwarten« - Passive Sicherheit

Komplexität verringern

Fehlerquellen reduzieren
Keine Hilfsmittel für Angreifer

Schadenswirkung einschränken

User-Rechte gering halten (nie Root)
Filesystem read-only
Filesystem »verkleinern« - chroot-jail

Detektieren

Integritätstest
Scannen

Maßnahme erfordert Konzept!

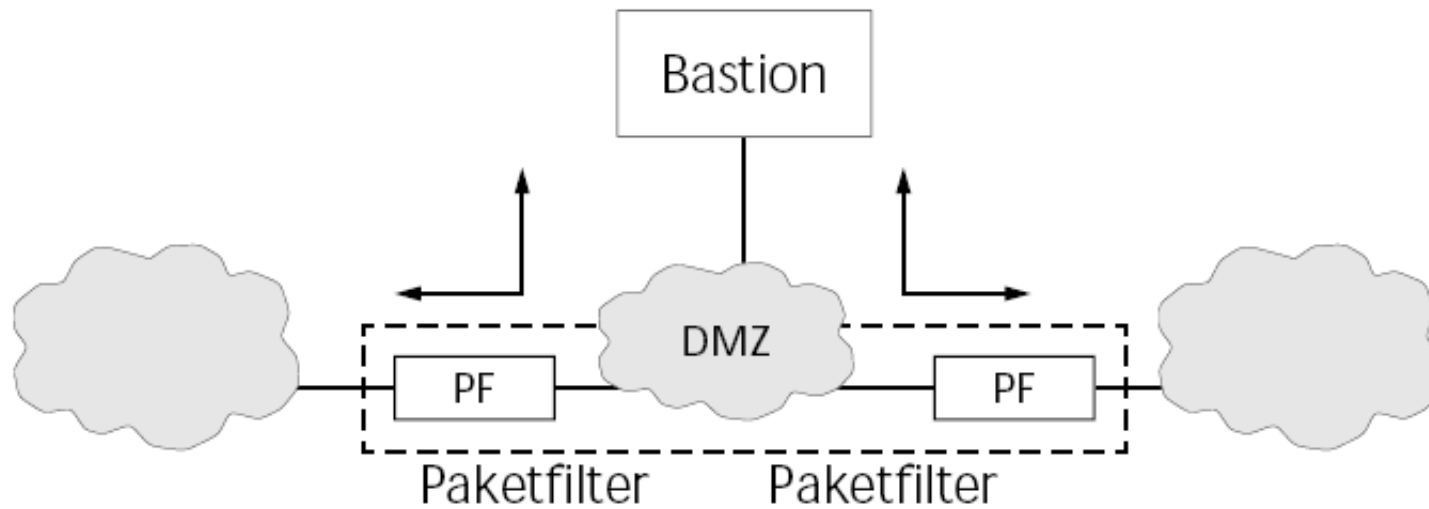
Firewalls

Definition	Kontrollierte Verbindung von Netzwerken
Funktion	Firewall=Konzept +Software + Hardware Policy bestimmt das Verhalten
Anforderungen	Stabiles, widerstandsfähiges System (gehärtet) Administration notwendig
Probleme	Komplexität erzeugt Angriffspunkte Schutz nur auf Basis von Netzwerkverbindungen Tunneling möglich, z.B. durch Verschlüsselung Nur Schutz gegen »Außen«
Ausprägungen	Hardwarefirewall – Appliances Personal Firewall

Einstufige Firewall

Inneres Netzwerk

Äußeres Netzwerk



Penetrationstest durch Security Scanner

Definition	Schwachstellensuche in Netzwerken
Funktion	Prüfung auf Vorhandensein von Angriffspunkten durch Scannen und Angreifen von Netzwerkdiensten
Anforderungen	Vertraulichkeit der Ergebnisse Administration notwendig
Probleme	Erkennung nur von bekannten Schwachstellen Preisgabe von Informationen bei externen Testern
Besonderheiten	Oft die gleichen Tools, die von Angreifern genutzt werden

Nessus

Architektur	Client-Server Betrieb auch auf einem einzelnen Rechner möglich Server nur für Unix-/Linux-Systeme Client auch für Windows Kommerziell/GPL-Version http://www.openvas.org/doku.php (GPL) http://www.nessus.org/ (Tenable Network Security, Inc.)
Schwachstellen werden erkannt durch	diverse Portscans Tests werden realisiert durch Plugins Plugins zielen auf versch. Schichten und Anwendungen externe Programme (nmap) können integriert werden
Referenz	Wird vom BSI empfohlen!

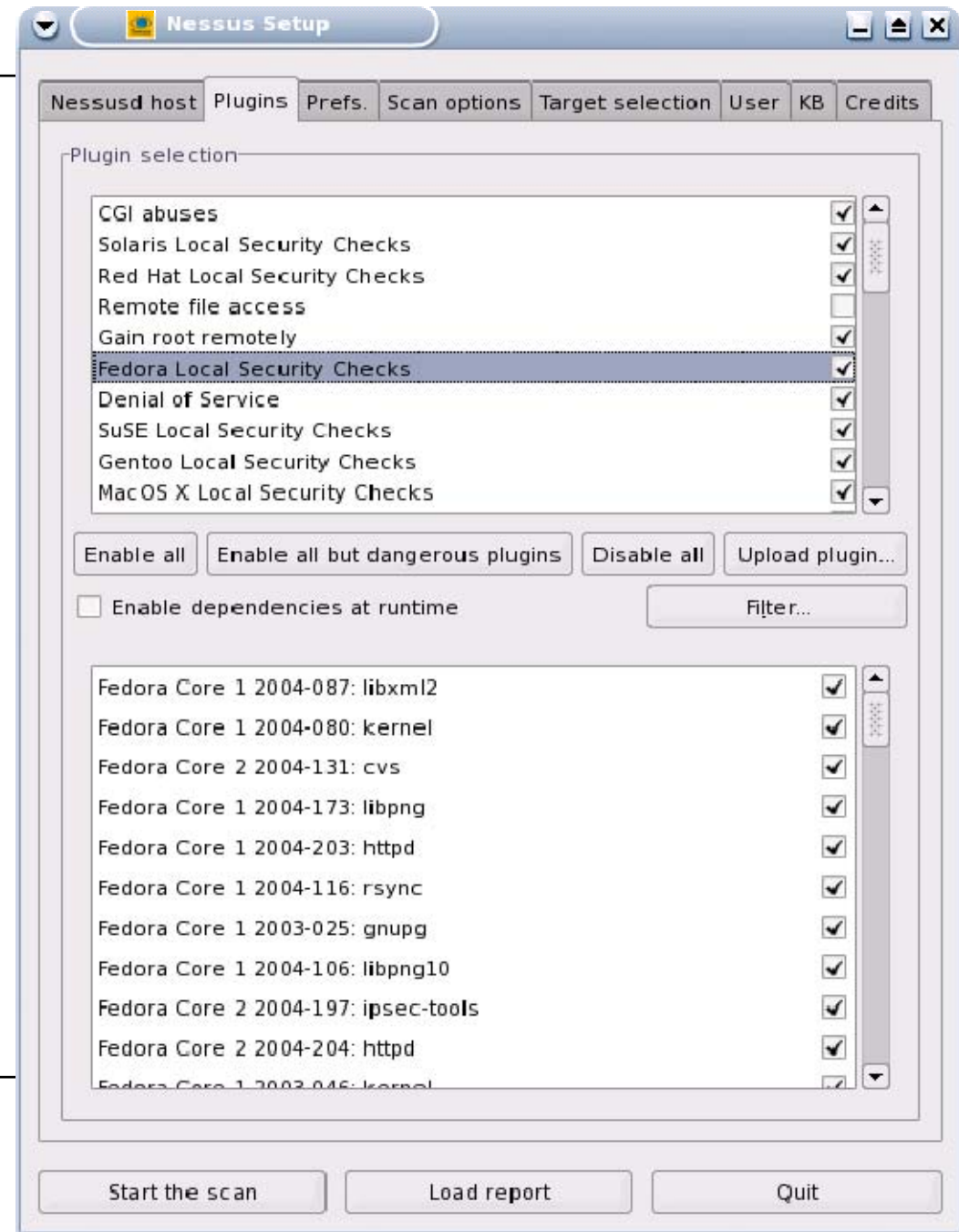
Nessus Plugins

Auswahl durchzuführender Plugins nach Kategorien

Funktionsbeschreibung zu jedem Plugin und Quellcode (proprietäre Skript-Sprache)

Kommerzieller Anbieter stellt derzeit mehr als 9000 Plugins bereit

Plugins verweisen immer auf bestimmte CVE IDs



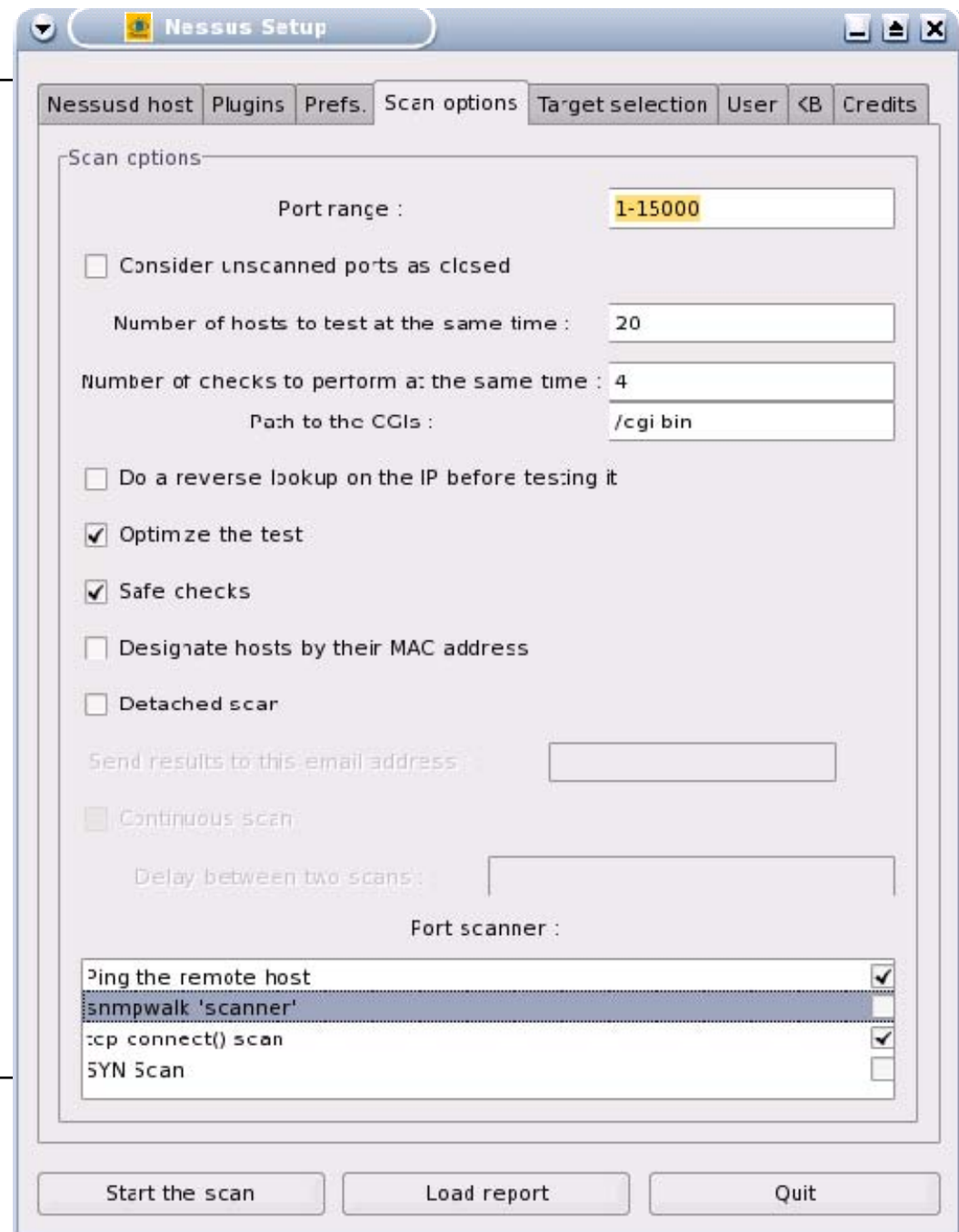
Nessus Scan Options

Ports variabel auswählbar

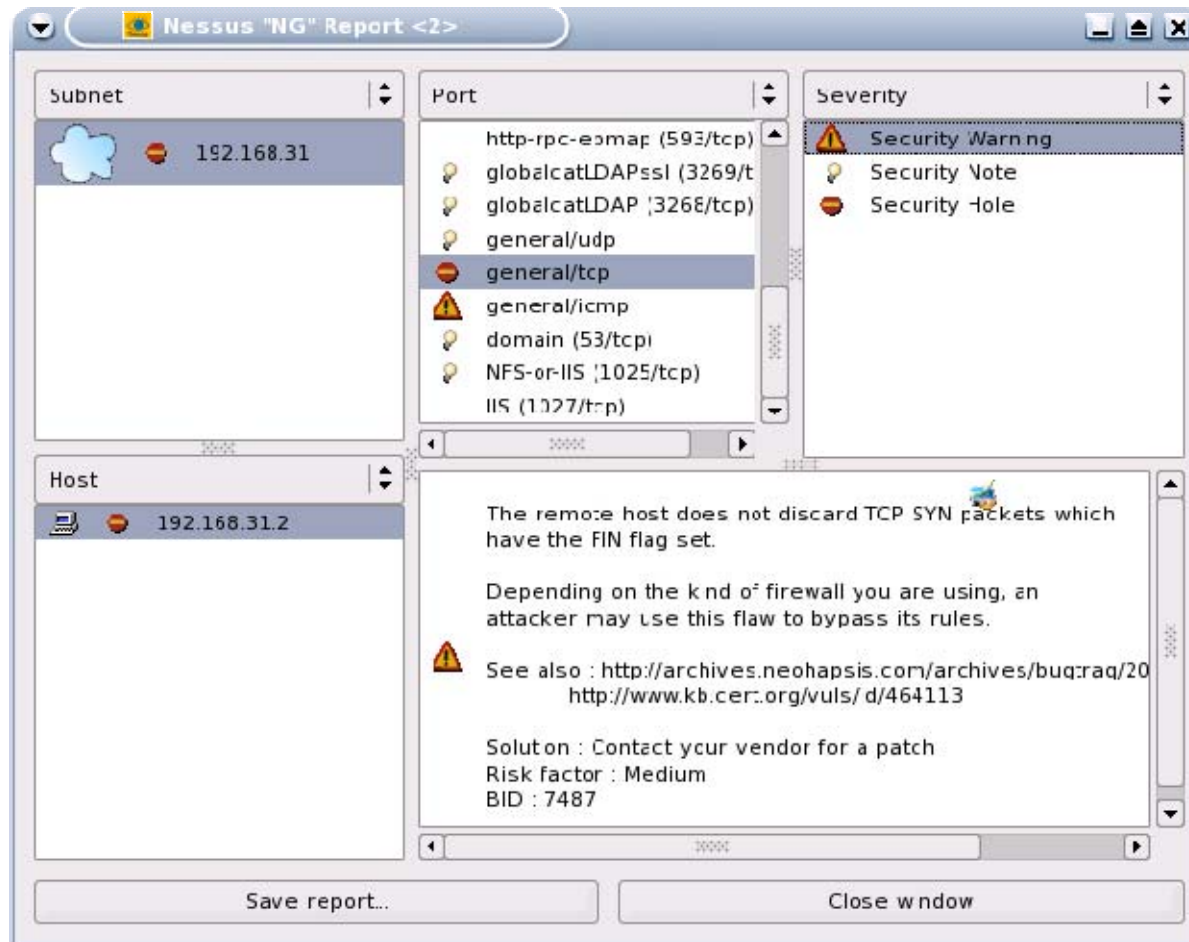
Anzahl der gleichzeitig zu testenden Hosts oder durchzuführenden Tests

Anpassen der Aggressivität

Auswahl der verfügbaren Portscanner



Nessus-Auswertung



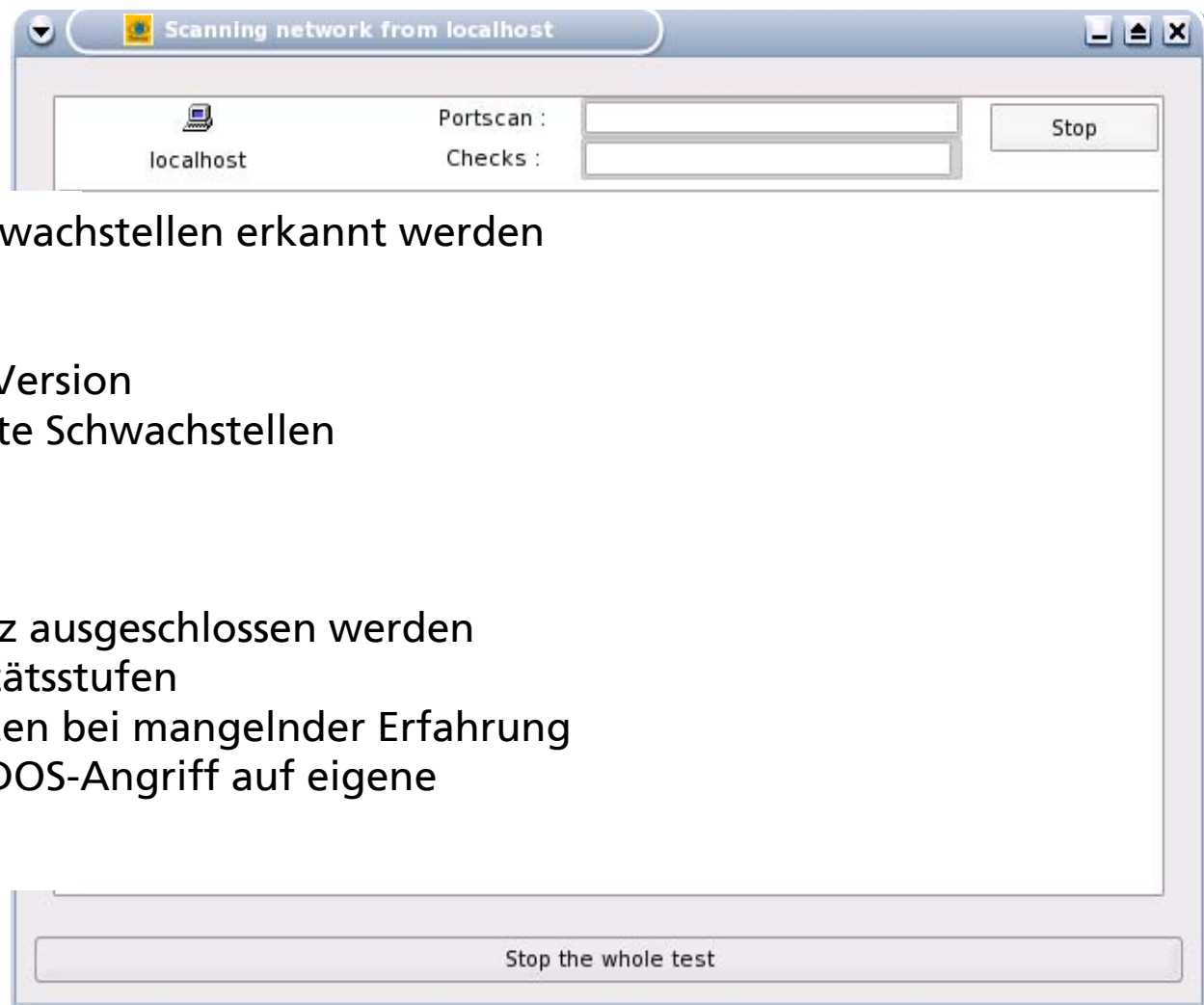
Übersichtliche
Auflistung der
durchsuchten Netze,
Hosts und gefundenen
Schwachstellen

Hinweise zur Art,
Schwere und Behebung
der Schwachstellen

Tatsächliche
Auswertung und
Umsetzung muss
manuell erfolgen



Nessus



Keine Garantie, dass alle Schwachstellen erkannt werden

- Aktualität der Plugins
- Kommerzielle und freie Version
- Neue, noch nicht erkannte Schwachstellen

Gefahren

- Schäden können nie ganz ausgeschlossen werden
- Verschiedene Aggressivitätsstufen
- Vorsicht bei großen Netzen bei mangelnder Erfahrung
Netzlast/Verfügbarkeit: DOS-Angriff auf eigene
Komponenten

Sicherheit als ganzheitlicher Ansatz (1)

Sicherheit als	Prozess Kette
Organisation	organisatorische Probleme lassen sich nicht durch Technik lösen Sicherheit ist Management-Aufgabe, Verantwortlichkeiten detailliert festlegen
Nachrüstung	kann zu erhöhten Investitionskosten führen Integration oft schwierig/lückenhaft
Besser	Sicherheitsanforderungen von vornherein berücksichtigen/einplanen

Sicherheit als ganzheitlicher Ansatz (2)

Maßnahmen

IT-Sicherheit ist ein Produktmerkmal im Einkauf
Fragestellungen im Entwicklungsprozess
Auswirkungen auf Architektur
IT-Sicherheit in Weiterbildung aufnehmen
Know-how in Standards nutzen

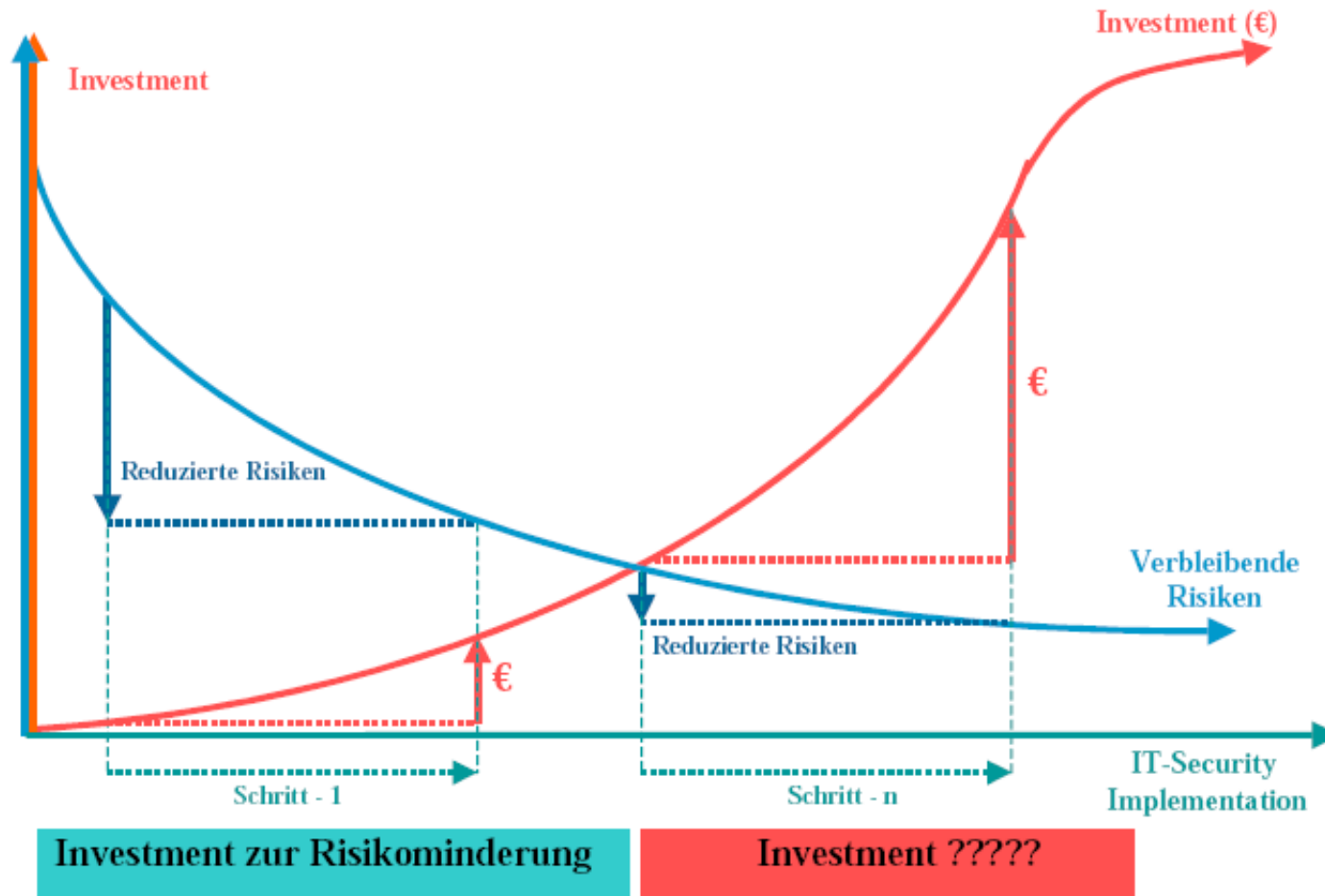
Standards

IT-Grundschutzhandbuch des Bundesamtes für
Sicherheit in der Informationstechnik (BSI)
BS7799, ISO 17799, ISO 27001, Common Criteria
(ISO/IEC 15408)

Kosten-Nutzen-Betrachtung bei IT-Sicherheit

Schadenskosten	Schäden vermeiden Bsp.: Rufschaden durch Verlust von Kreditkartendaten
Kostenquellen	Rückrufaktion, Kulanz, Kundenverlust, Versicherer, Zulieferer, Compliance, Anforderungen durch Banken (Bsp. Basel II)
Kosten	Kreditwürdigkeit, Zins, Prämien, Auftragsverlust
Wettbewerbsfähigkeit	Wirtschaftliche Betriebsführung Effizienz

IT Sicherheitsrisiken und -investment



Quelle: Prof. Dr. Norbert Pohlmann, Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsmechanismen



Vorgehen nach BSI

Schritte

1. Erstellung einer IT-Sicherheitsleitlinie
2. Auswahl und Etablierung einer geeigneten Organisationsstruktur für IT-Sicherheit
3. Erstellung einer Übersicht über vorhandene IT-Systeme
4. Erstellung des IT-Sicherheitskonzepts (Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Basissicherheitscheck, ergänzende Sicherheitsanalyse)
5. Umsetzung der IT-Sicherheitsmaßnahmen
6. IT-Sicherheit im laufendem Betrieb
7. Aufrechterhalten des sicheren Betriebs

<http://www.bsi.de/>



Vielen Dank!

Kontakt

Fraunhofer Institut für
Software- und Systemtechnik (ISST)
<http://www.isst.fraunhofer.de>

Abteilung Sichere Business IT-Systeme
Malte Timmermann

Tel.: 030 / 24306 – 441

Mail: [Malte.Timmermann @ isst.fraunhofer.de](mailto:Malte.Timmermann@isst.fraunhofer.de)