
eSI - Der elektronische Sicherheitsinspektor

Unterstützung für eine kontinuierliche
Überprüfung von IT-Sicherheitsmaßnahmen
in Unternehmensnetzen

Michael Zapf

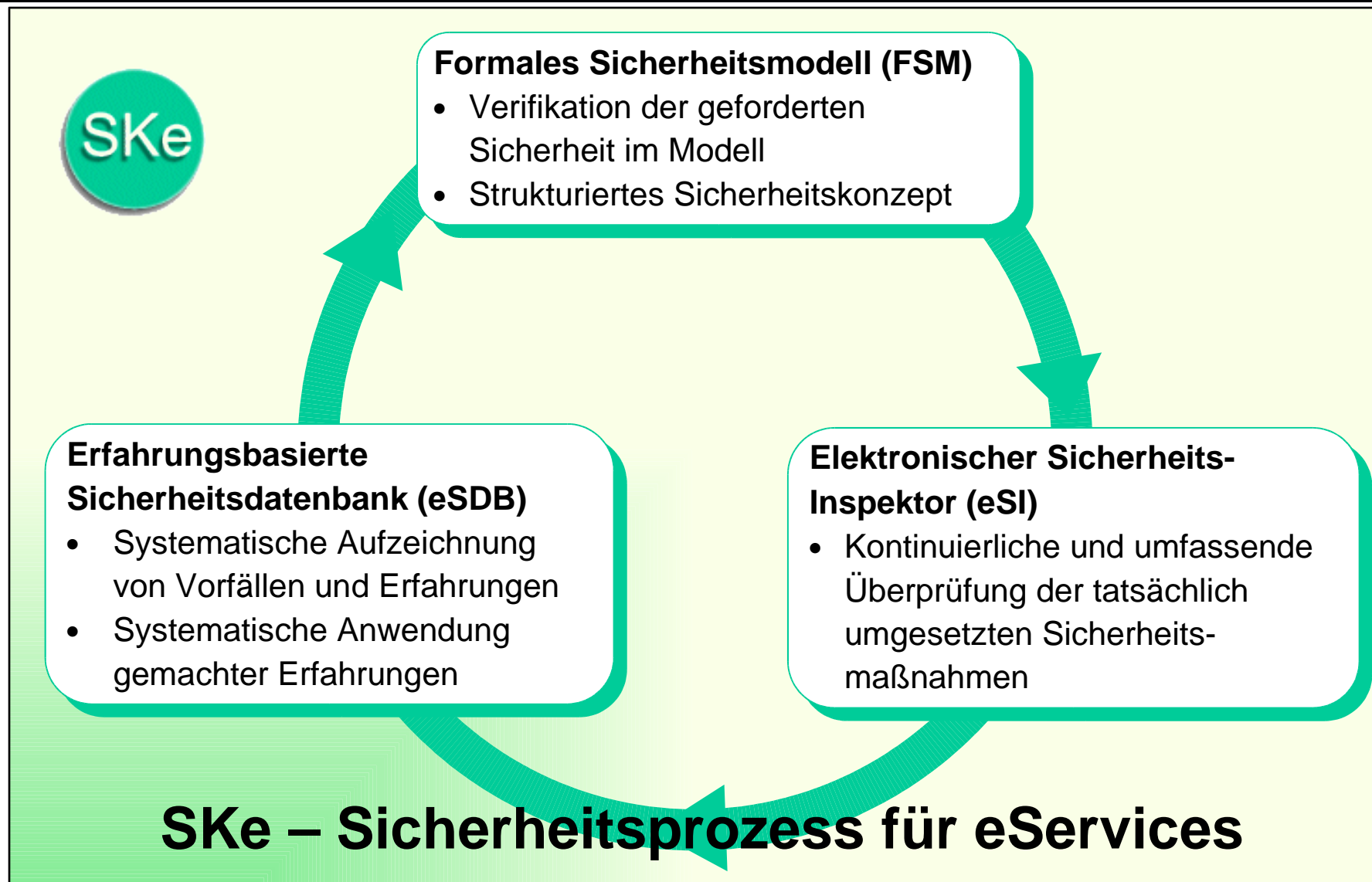
Überblick

- eSI im Projekt SKe
- IT-Sicherheitsmaßnahmen
- Werkzeugeinordnung des eSI
- eSI - Vorgehensmodell zur automatisierten Überprüfung
- eSI - Komponenten / Funktionen
- eSI - Maßnahmenüberprüfungen
- eSI - Einsatzszenarien
- Zusammenfassung



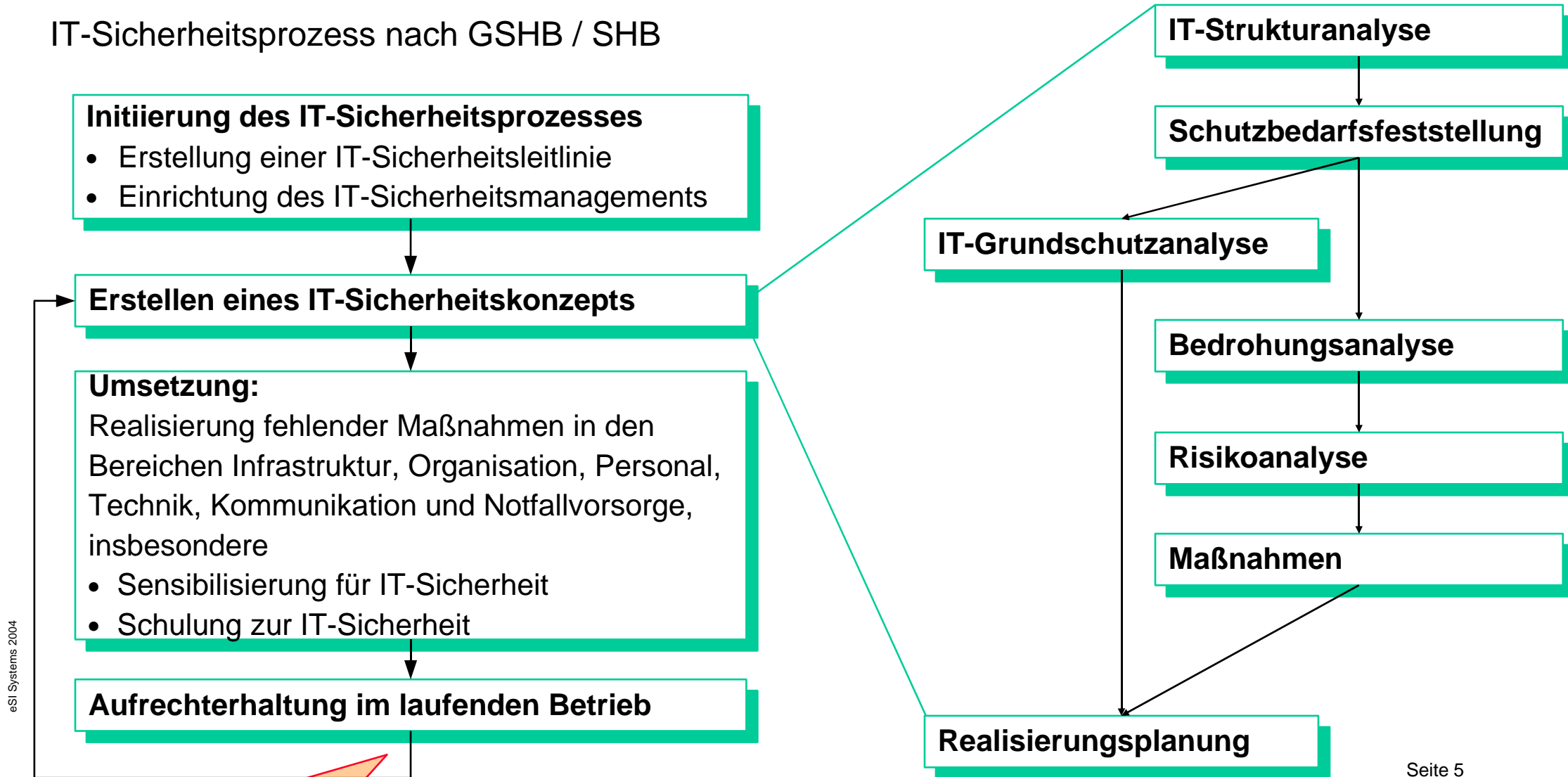
- SKe „Durchgängige Sicherheitskonzeption mit dynamischen Kontrollmechanismen für eService-Prozesse“.
Ein BMBF-Förderprojekt im Programm „Leben und Arbeiten in einer vernetzten Welt“ (Mai 2001 bis Dezember 2003) mit folgenden Teilprojekten:
 - Formales Sicherheitsmodell, Angriffsimulator, strukturiertes Sicherheitskonzept
 - elektronischer Sicherheitsinspektor eSI
 - Erfahrungsbasierte Sicherheitsdatenbank, Aufzeichnen von Vorfällen, Diagnose von Vorfällen, Handlungsempfehlungen

eSI im Projekt SKe



IT-Sicherheitsmaßnahmen

IT-Sicherheitsprozess nach GSHB / SHB



eSI Systems 2004

Werkzeugunterstützung durch eSI

Werkzeugeinordnung des eSI

Existierende Werkzeuge für:

- Erstellen von Sicherheitskonzepten (GSTOOL, „textorientiert“)
- Umsetzung von IT-Sicherheitsmaßnahmen
 - teils händisch, teils Werkzeug-unterstützt
 - teils automatisierte Umsetzung bei Produkt-bezogener Konfiguration (Policy enforcement: Windows-Richtlinien, ePolicy Orchestrator)
- Überprüfung auf Schwachstellen (Vulnerability scanner: „Baseline Security Scanner“, Nessus)
 - Bekannte Programmfehler (bugs) in Standardprodukten (Server, PCs, E-Mail...)
 - Bekannte Konfigurationsfehler in Standardprodukten (Server, PCs, E-Mail...)
- Überprüfung von IT-Sicherheitsmaßnahmen (Sicherheitsaudit,...)



Werkzeugeinordnung des eSI



- z. B. Security Audit 2003/2004
 - Checklisten für Interviews, Begehungen, Security Scans
 - ...„Jede Checkliste enthält außer den durchzuführenden Arbeiten ein Bewertungsschema, um den Erfüllungsgrad jeder Prüfung zu messen. Zusätzlich gibt es K.O.-Kriterien, ohne deren Bestehen das Fazit einer Prüfung „durchgefallen“ lautet.“...
 - Mitgelieferte Werkzeuge
 - Portscanner: nmap (Unix), MingSweeper (Windows)
 - Security-Scanner: nessus (Unix), LANguard Network Security Scanner (Windows), N-Stealth (Windows-Tool für den Scan von Webservern)
 - Integritäts-Checker: AIDE (Unix), Tiger (Unix)
 - Prüfung von Passwörtern: LC4 (Windows), Crack (Unix)
 - Registry-Tools: doeskey (Windows)



Werkzeugeinordnung des eSI

- z.B. Prüfschema für Auditoren (BSI, Qualifizierung/Zertifizierung nach IT-Grundschutz)
- Überprüfung „nach Aktenlage“ (Referenzdokumente)
- Inspektion vor Ort
 - „Der Auditor überprüft vor Ort die Umsetzung aller Maßnahmen des Bausteins „IT-Sicherheitsmanagement“ für den IT-Verbund.“
 - Zusätzlich zur Überprüfung des Management-Bausteines sind **Stichproben** aus den fünf Schichten "Übergeordnete Aspekte", "Infrastruktur", "IT-Systeme", "Netze" und "Anwendungen" zu wählen.“

eSI - Der elektronische Sicherheitsinspektor

**Der elektronische Sicherheitsinspektor (eSI)
kontrolliert die Einhaltung der IT-Sicherheitsmaßnahmen / - Richtlinien**

Mit Hilfe von elektronischen Checklisten kann eine derartige Überprüfung

- kontinuierlich,
- umfassend (nicht nur Stichproben) und
- automatisiert

durchgeführt werden.

Welche Maßnahmen sind automatisiert überprüfbar?

- Technische Maßnahmen: grundsätzlich ja
- Organisatorische Maßnahmen (Richtlinien) im Einzelfall
 - „Auf den Arbeitsplatzrechnern dürfen keine privaten Programme installiert werden“: eher ja
 - „Die Mitarbeiter sind über die aktuellen Datenschutzrichtlinien zu informieren“: eher nein



Prüfverfahren für Maßnahmen

- „Verhaltensprüfung“ des Objekts (tut es, was es tun soll?)
- Konfigurationsprüfung (korrekte Konfiguration bewirkt korrektes Verhalten)

Prüfwerkzeugimplementierung

- Zentrale Implementierung (etwa Portscanner)
- Verteilte Implementierung (etwa zentraler Abruf der Messwerte von lokal installierten „Agenten“)

Welche Maßnahmen werden vom eSI überprüft?

- „Standard-Maßnahmen“
 - Grundschutzhandbuch
 - SANS Top 20
- Individuelle Maßnahmen
 - Unternehmens- / anwendungsspezifisch

eSI - Vorgehensmodell zur automatisierten Überprüfung

Schritt 1

- Person prüft mit Hilfe eines „Standard- / Spezialwerkzeugs“ die korrekte Umsetzung / Einhaltung einer Maßnahme
 - Gliederung in zu prüfende Teilmaßnahmen
 - Kriterien für Umsetzung bestimmen (zu prüfende Messwerte, „Messstellen“, „Qualität“)
 - Werkzeug auswählen
 - Bedienung lernen
 - Prüfauftrag eingeben
 - Prüfergebnisse interpretieren und auswerten

eSI - Vorgehensmodell zur automatisierten Überprüfung

Schritt 1

Wissen über

- den Umgang mit Sicherheitsmaßnahmen
- die Prüfung von Umsetzungszuständen
- Umgang mit Prüfwerkzeugen
- die Interpretation der Prüfergebnisse und der Auswertungsergebnisse



Sicherheitsbeauftragter
Sicherheitsaudit /-revision



Prüfwerkzeug

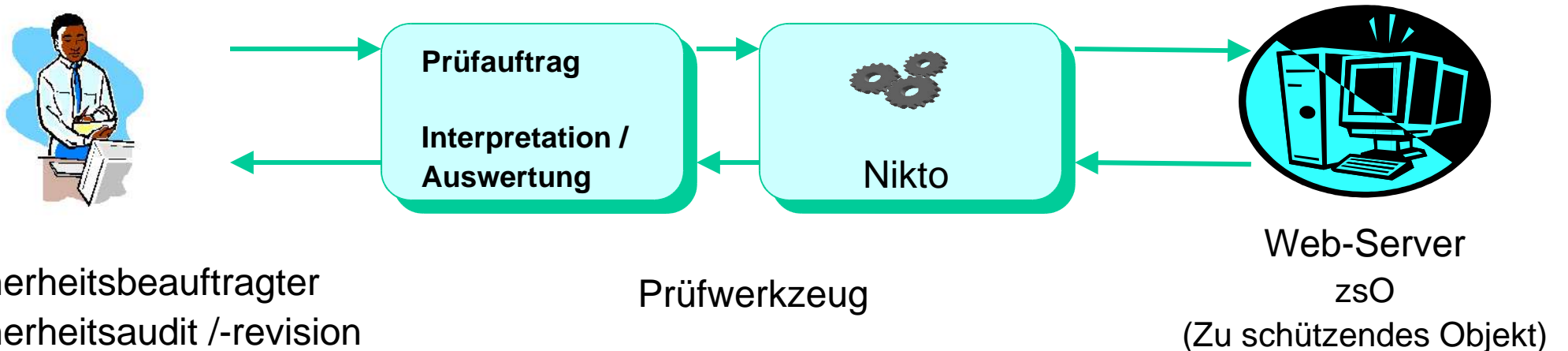


Web-Server
zsO
(Zu schützendes Objekt)

eSI - Vorgehensmodell zur automatisierten Überprüfung

Schritt 2

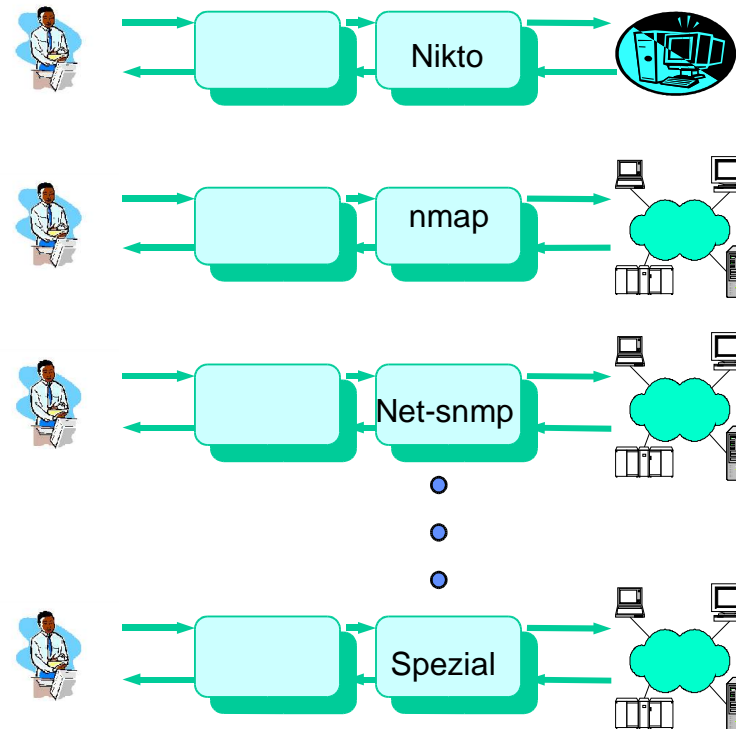
- Prüfauftrag automatisieren (welche Maßnahme, welches Objekt, wann...)
- Automatisierte Interpretation und Auswertung der Ergebnisse



eSI - Vorgehensmodell zur automatisierten Überprüfung

Schritt 3

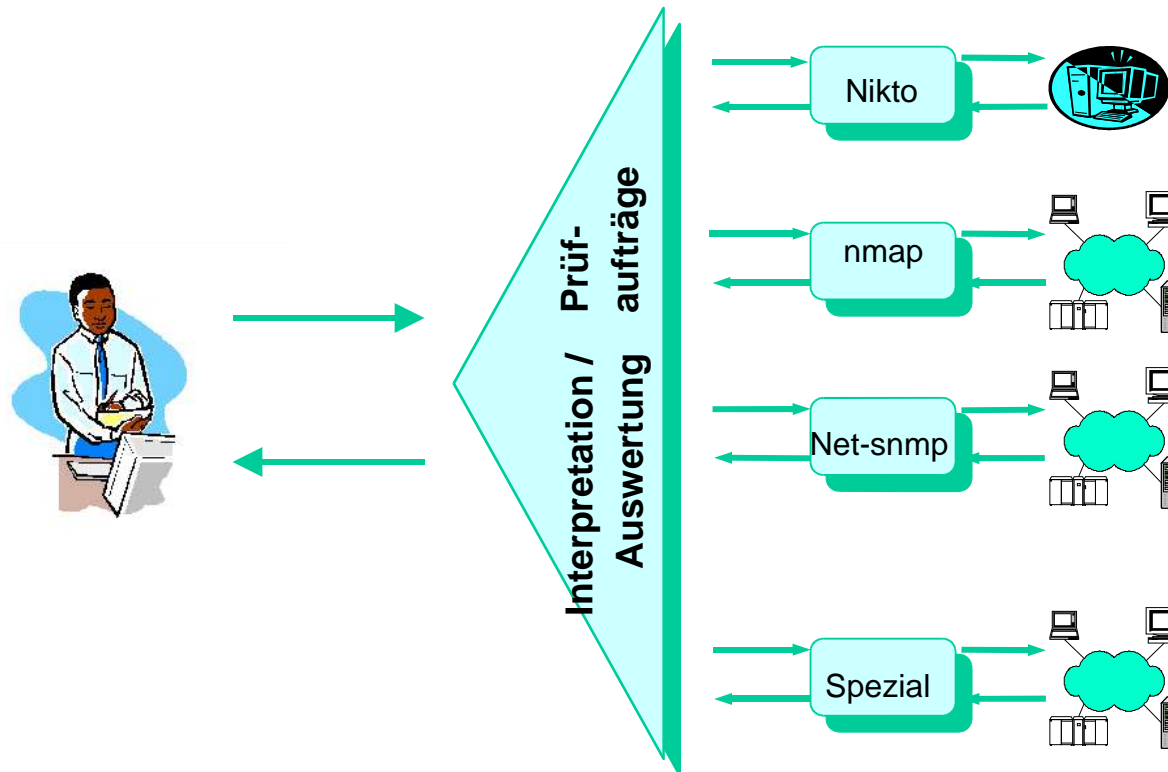
- Viele Werkzeuge für unterschiedlichste Prüfzwecke / Maßnahmen



eSI - Vorgehensmodell zur automatisierten Überprüfung

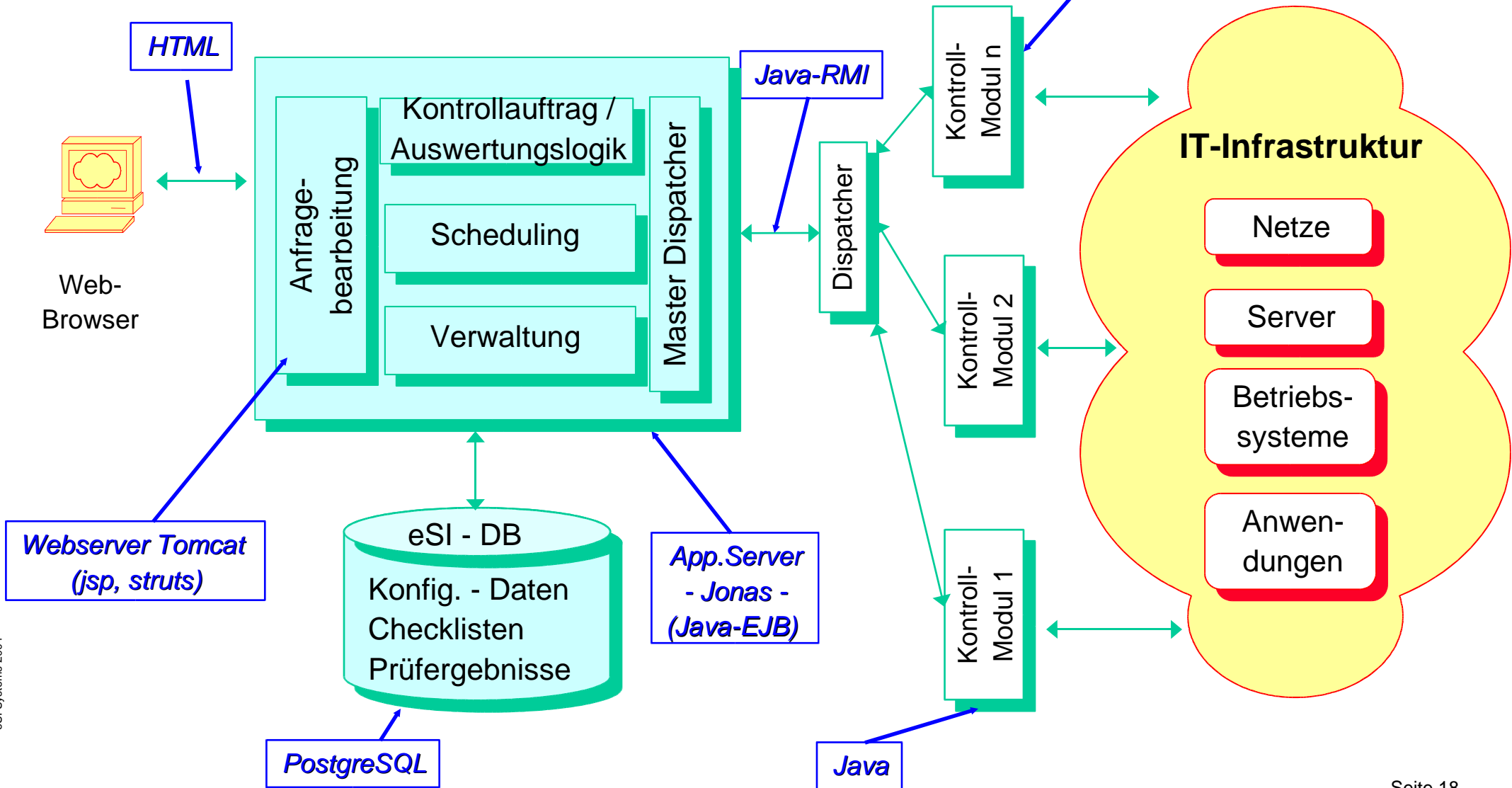
Schritt 4

- Ein Zugangspunkt und einheitliche Bedienung für alle Prüfwerkzeuge



eSI-Komponenten

Prüfwerkzeuge (Nikto, Nmap, NBTscan, SSL/TLS, Net-SNMP, Win-Registry, Stringsuche in Dateien,...)



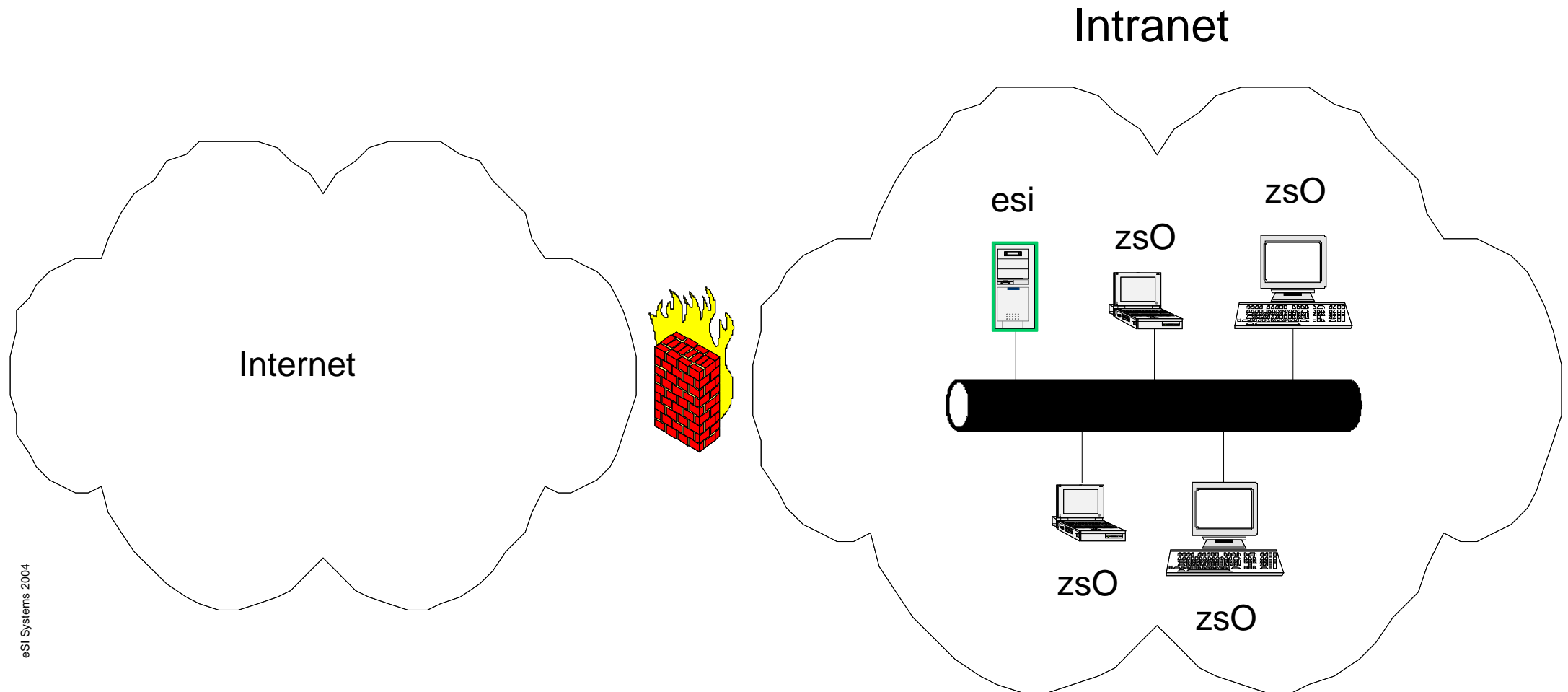
Einige eSI-Maßnahmenüberprüfungen

Einige Maßnahmen-Beispiele:

- „Abschalten von DNS“ GSHB M4.96 V07/99
- „Ein Dienst pro Server“ GSHB M4.97 V07/99
- „Standardscripte“ entfernen <=> MnNr.5 SANS G7 V2.504
- „Port 111 (RPC) blockieren“ SANS U1 V3.21
- „Problematische Parameter bei Samba“ GSHB M5.82 V10/00
- „regelm. Aktualisierung des Virensuchprogr.“ GSHB M4.3 V07/99
- „Entfernen des »Button Herunterfahren«“ GSHB M4.175 V10/03
- „residenter Betrieb des Virensuchprogramms“ GSHB M4.3 V07/99
- „Virens Scannerkonfiguration nach Vorgabe“ Spezial-SKE M0.006
- „»Verzeichnisinhalt auflisten« deaktivieren“ GSHB M2.174 V10/03
- „Symbolische Links deaktivieren“ GSHB M2.174 V10/03
- „IP-Forwarding deaktivieren“ GSHB M4.95 V07/99

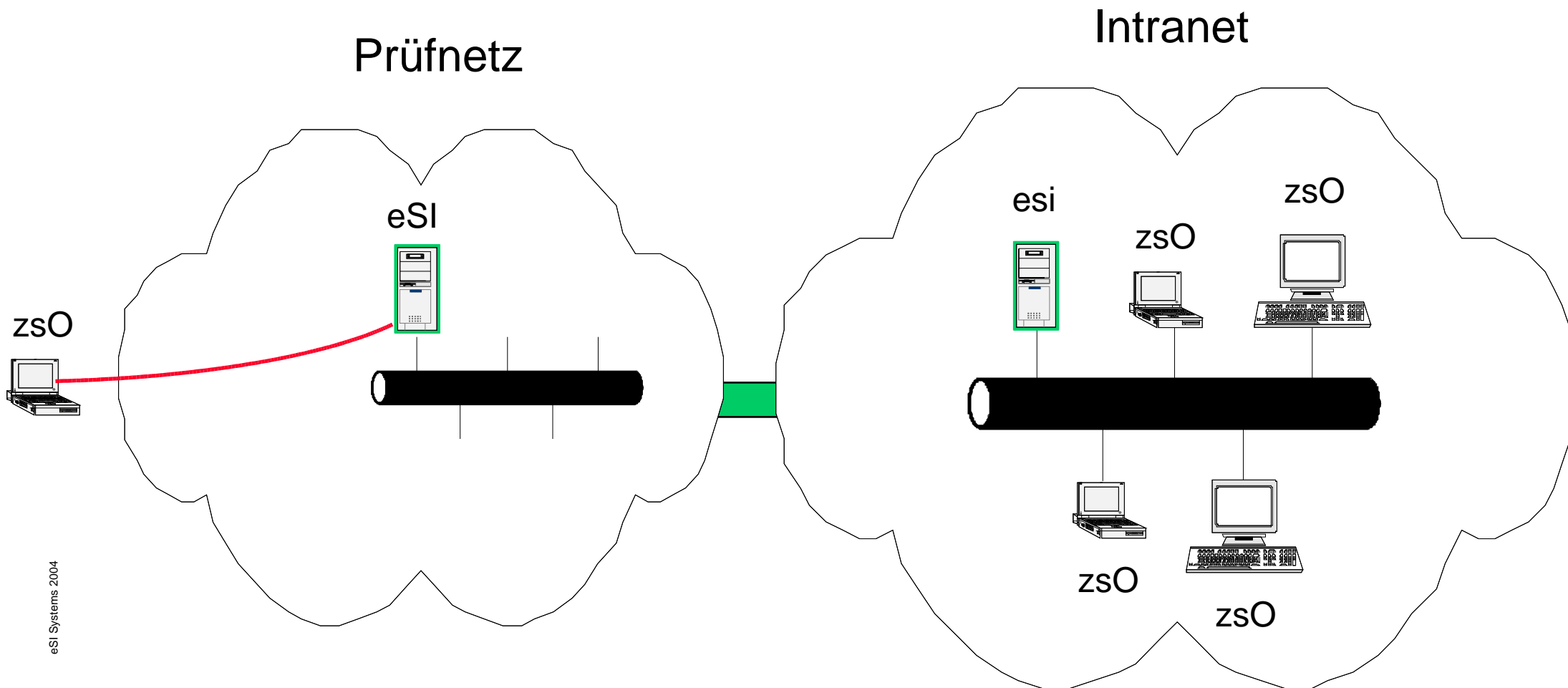


eSI-Einsatzszenarien Intranet



eSI Systems 2004

eSI-Einsatzszenarien Zugangsprüfung



eSI Systems 2004

Zusammenfassung

Der elektronische Sicherheitsinspektor (eSI) kontrolliert die Einhaltung der IT-Sicherheitsmaßnahmen / - Richtlinien

- kontinuierlich
- umfassend (nicht nur Stichproben)
- automatisiert

- Er liefert einen kontinuierlichen „SOLL–IST“-Vergleich zwischen
- angestrebtem Sicherheitsniveau und
- tatsächlichem Sicherheitsniveau



Gefahren kennen

Risiken minimieren

Chancen nutzen



Kontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Bereich Sichere Prozesse und Infrastrukturen

Dr. Michael Zapf

Rheinstraße 75
D-64295 Darmstadt

Telefon: +49-6151-869-60024
Telefax: +49-6151-869-224

Michael.Zapf@sit.fraunhofer.de

<http://www.sit.fraunhofer.de>

