Der Einsatz eines Security-Scanners in einem globalen Unternehmen

Dirk Lehmann
Siemens CT IC 3, Security Technologies
Siemens CERT

Dirk.Lehmann@cert.siemens.de

Agenda (1)

- Einleitung
  - Warum Scannen?
- Einsatzszenarien
  - Große vs. kleine Rechnerlandschaft
  - Zentral vs. dezentral durchgeführte Scans
  - Regelung der Verantwortung bei einem Scan
  - Restriktive Vergabe der Scan-Berechtigung
  - Untersuchungszeitpunkte
- Aufbau und Konfiguration eines Scan-Rechners

Agenda (2)

- Durchführung eines Scan – Best Practices
  - Planung eines Scans – die Scan-Policy
  - Identifizierung der Zielsysteme
  - Scan der Zielsysteme
- Auswertung des Scan-Ergebnisses
- Zusammenfassung
- Diskussion

Einleitung

- Bedrohungslage
  - Hacker-Einbruch bei MS, Einbruch bei WEF
  - Erpressung durch Hacker (NIPC)
- Security-Scanner
  - „Wie ein Hacker“
  - Pro-aktiv
  - Schnappschuß der Sicherheitslage
  - regelmäßige Updates wichtig

Einsatzszenarien: Große vs. kleine Rechnerlandschaft

- Vorteile beim Scannen eines kleinen überschaubaren Rechnernetzes
  - Kritische Produktivsysteme bekannt
  - Administratoren kritischer Systeme bekannt
  - Keine unbekannten Geräte
  - Systeme anderer Einheit im eigenen IP-Adreßband wahrscheinlich bekannt
  - Administratoren bekannt, die Patches installieren müssen
  - Scan-Manager u.U. selbst Administrator

Einsatzszenarien: Große vs. kleine Rechnerlandschaft

- Nachteile beim Scannen eines großen unübersichtlichen Rechnernetzes
  - Kritische Produktivsysteme unbekannt, Abstimmungsbedarf mit vielen Administratoren
  - Scannen fremder Systeme schwer vermeidbar (Reorganisation)
  - Unbekannt Geräte (andere Einheit, altes System, Fremdkörper?)
  - Patchen der Schwachstellen problematisch, da Scan-Manager nicht Systemverantwortlicher

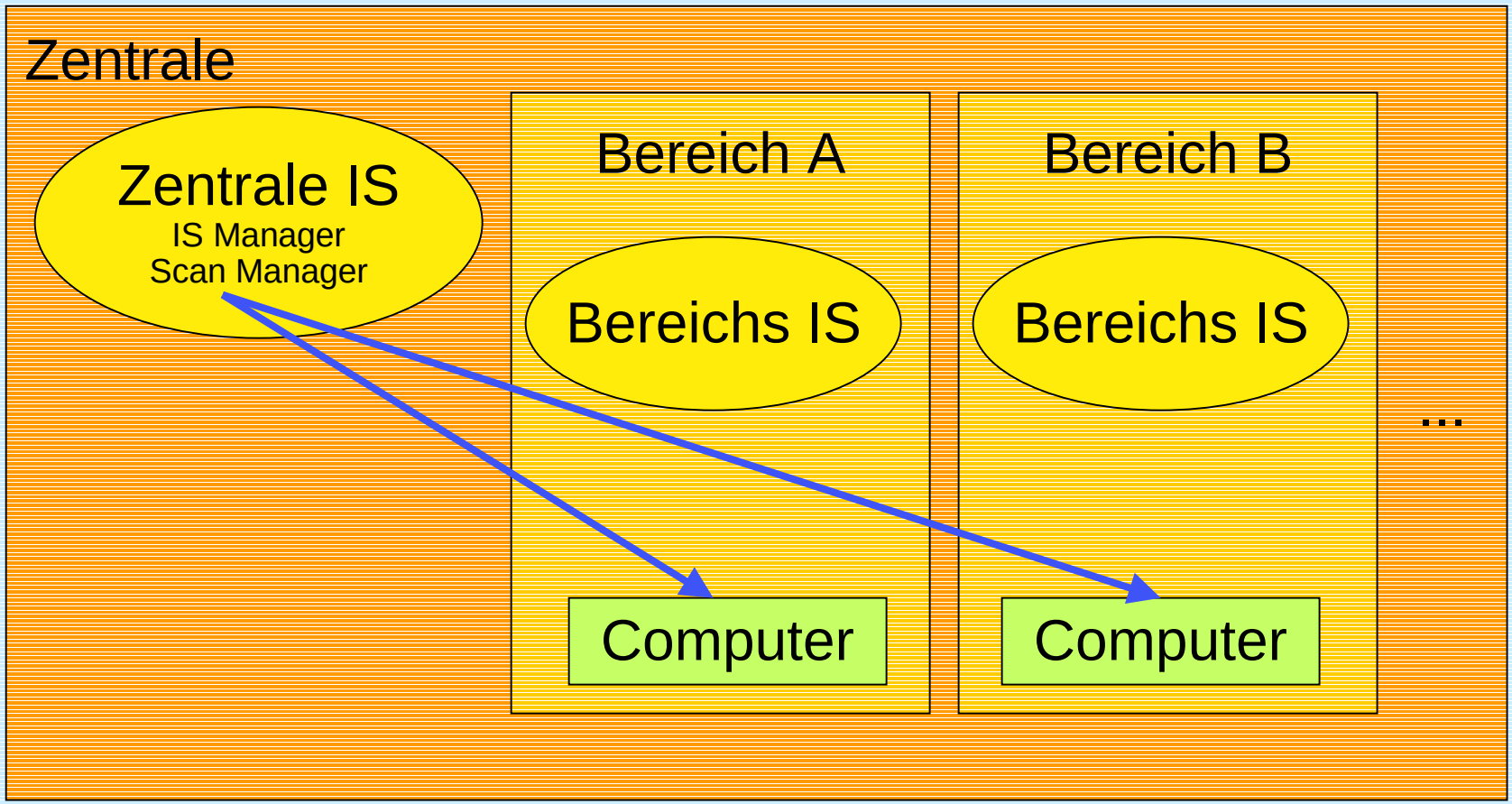
Einsatzszenarien: Zentral vs. dezentral durchgeführte Scans

- Dezentrale bzw. lokale Scans haben die Vorteile einer kleinen Rechnerlandschaft
  - Kein Konflikt zwischen Schwachstelle beseitigen und Betrieb nicht stören
- Zentrale Scans
  - Übersicht über alle Systeme
  - Erreichung eines einheitlichen Sicherheitsniveaus
  - Nur Stichproben möglich
  - Gefährliche Untersuchungen weglassen (DoS)
  - Überprüfung eines geringeren Sicherheitsniveaus als ein dezentraler Scan
  - Unabdingbar für Qualitätssicherung

Regelung der Verantwortung bei einem Scan

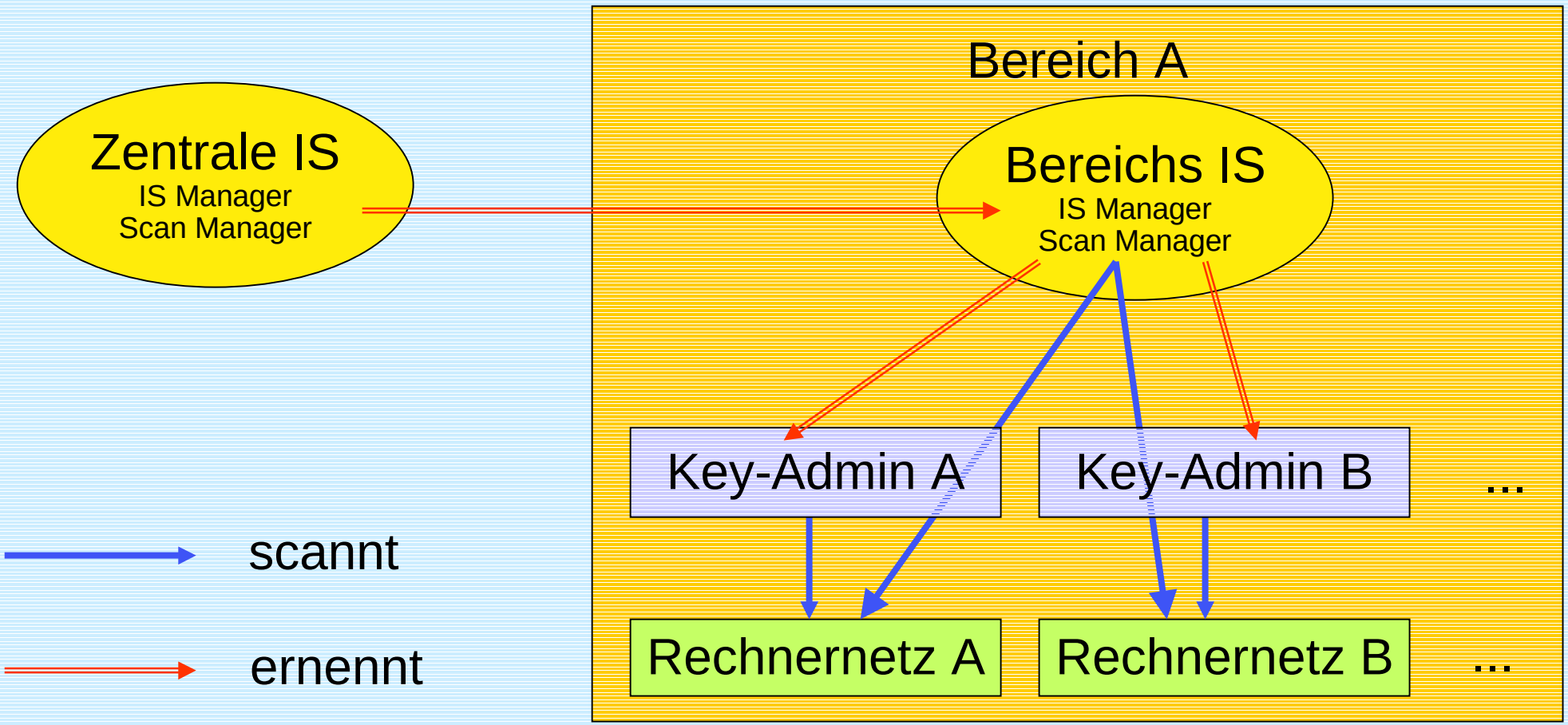
- Dezentraler Scan
  - Zentrale IS-Abteilung ernennt Scan-Manager
  - Scan-Manager ernennt Key-Administratoren
  - Key-Administratoren scannen ihre Systeme
  - Scan-Manager macht Audit-Scan
- Zentraler Scan
  - Zentrale IS-Abteilung macht Stichproben

Regelung der Verantwortung bei einem Scan: zentraler Scan



s

Regelung der Verantwortung bei einem Scan: dezentraler Scan



Restriktive Vergabe der Scan-Berechtigung

- Ein Scanner ist ein mächtiges Werkzeug
  - Was tut jemand mit dem gewonnen Wissen über Schwachstellen?
  - Jeder sollte nur das Scannen können, wozu er eine Berechtigung besitzt.
  - Lizenzserver gestattet nur authorisierten Personen den Zugriff
  - Jeder kann nur Lizenzen für sein eigenes Rechnernetz erwerben
  - Lizenzen sollten zeitlich limitiert sein

Untersuchungszeitpunkte

- Untersuchungszeitpunkt beeinflußt Ergebnis
  - Erster Scan überhaupt wird enorm viele Schwachstellen finden
    - Behebung priorisieren
  - Tageszeit
  - Unerreichte Systeme müssen unbedingt beim nächsten Scan erreicht werden
- „Sichere Systeme“ werden im laufenden Betrieb wieder unsicher
  - Scanner-Einsatz muß kontinuierlich sein
  - Jährliche Revisions-Scans aller Rechner
  - Quartalsmäßige Überprüfungen der Systeme in den Bereichen
  - Monatliche Scans der Key-Administratoren

Untersuchungszeitpunkte

- „Frische“ Systeme untersuchen, bevor sie ans Netz gehen
  - Scanner wird regelmäßig vom Hersteller aktualisiert
  - Neueste Schwachstelle von Installationsanleitung berücksichtigt?
  - Qualitätskontrolle für Installateur
- Schwachstellen müssen vor nächstem Scan behoben sein
  - Kontrolluntersuchung mit identischer Scanner-Konfiguration
  - Nächster regulärer Scan mit aktualisierter Scanner-Version
- Außerplanmäßiger Scan bei Erhalt einer aktualisierten Scanner-Version

Aufbau und Konfiguration eines Scan-Rechners

- Dediziertes System
  - Schutz vor verfälschten Ergebnissen
  - Scanner kann andere Arbeit nicht beeinträchtigen
- Höchste Sicherheitsanforderungen
  - Scanner sammelt die Infos, die jeder Hacker gerne hätte
  - Netzverbindung physikalisch trennen, so lange nicht gescannt wird
  - Scan-Ergebnisse verschlüsseln
  - Email-Verschlüsselungssoftware

Planung eines Scans – die Scan-Policy

- Design und Implementierung einer Scan-Policy
  - Steuert den Scan-Ablauf
- Vorsicht vor DoS-Schwachstellenüberprüfungen
- Trennung in Windows- und UNIX-Checks
- Menge der Schwachstellen-Checks begrenzen
- Verschiedene Policies für unterschiedliche Sicherheitsanforderungen festlegen
  - Z.B. alle Checks gegen FW, Internet-Systeme einsetzen
- Nicht alle Features eines Scanners nutzen
  - PW-Qualität am Besten mit Spezial-Tool überprüfen

Identifizierung der Zielsysteme

- Zielsysteme klassifizieren (Mission Critical System, einfache Workstation, Produktivsystem, Testrechner)
  - Scan-Policy und –Zeitpunkt darauf abstimmen
  - Risikopotential bestimmen und Systeme mit hohem Risiko zuerst scannen
  - Unkritische Systeme wie z.B. Drucker zuerst auslassen
- Discovery-Modus nutzen zum Auffinden aller Systeme
  - Einfachen Scan durchführen zur Identifikation des Typs
  - NMAP/QueSO können den Stack durcheinanderbringen
  - Alternativ Abgleich mit Inventarliste
- Immer wieder nach unbekannten Systemen suchen

Scan der Zielsysteme

- Mindestens 75% aller Systeme scannen
- Lange Scan-Dauer bei großem Netz einkalkulieren
  - Nicht Freitagabend einen Scan starten
- Niemals unbeaufsichtigt scannen
  - „Opfer“ informieren, daß gescannt wird
- NetBIOS- und DNS-Namen protokollieren

Auswertung des Scan-Ergebnisses

- Berichte erstellen mit unterschiedlichen Details für
  - Management, Mittleres Management, Techniker
  - Zahl der Schwachstellen insgesamt, pro System, Art der Schwachstelle, wie behebbar
- Ursachen dafür, daß eine Schwachstelle bei einem System immer wieder gemeldet wird
  - Kein Patch verfügbar
  - Patch behebt Problem nicht
  - Patch nicht einspielbar, da installierte SW nur bis Patchlevel XY freigegeben
  - Administratoren weigern sich, Patch einzuspielen („never touch a running system“)
  - Administratoren glauben nicht, daß Schwachstelle ausnutzbar

Auswertung des Scan-Ergebnisses

- Patch nie ungetestet einspielen
- Jede Schwachstelle verifizieren
  - False Positives dem Hersteller melden
  - Liste aller bekannten False Positives führen
- Was, wenn eine Backdoor gefunden wurde?
  - IRT verständigen
- Exponiertes System hat viele Schwachstellen
  - Neu aufsetzen
  - IRT verständigen

Zusammenfassung

- Verantwortlichkeit für Scans muß geregelt sein
- Scans müssen kontinuierlich durchgeführt werden
- Scan-Rechner muß sicher sein
- Konzernweite Scan-Policy sollte das Sicherheitsminimum definieren
- Möglichst lokal scannen, die Administratoren einbinden
- Scan-Ergebnisse nach oben und unten kommunizieren
- Nicht blind patchen