Musterpräsentation TOsecurity Audit

Die nachfolgenden Präsentationsfolien sind beispielhaft und dienen nur zur Veranschaulichung.

Die tatsächliche Ausprägung in Art und Umfang orientiert sich am jeweiligen Fokus des Security Audits sowie dem Teilnehmerkreis.

Im genannten Beispiel wurden zwei wertschöpfungsrelevante Server-Systeme auditiert.
Grundlage: ISO 27000-Familie, BSI IT-Grundschutz, Betriebssystem-Security-Policies des Herstellers IBM sowie kundenspezifische Regelwerke.

Policybased Security Audit

Kernprozesse Entwicklung/Produktion
IBM AIX Server

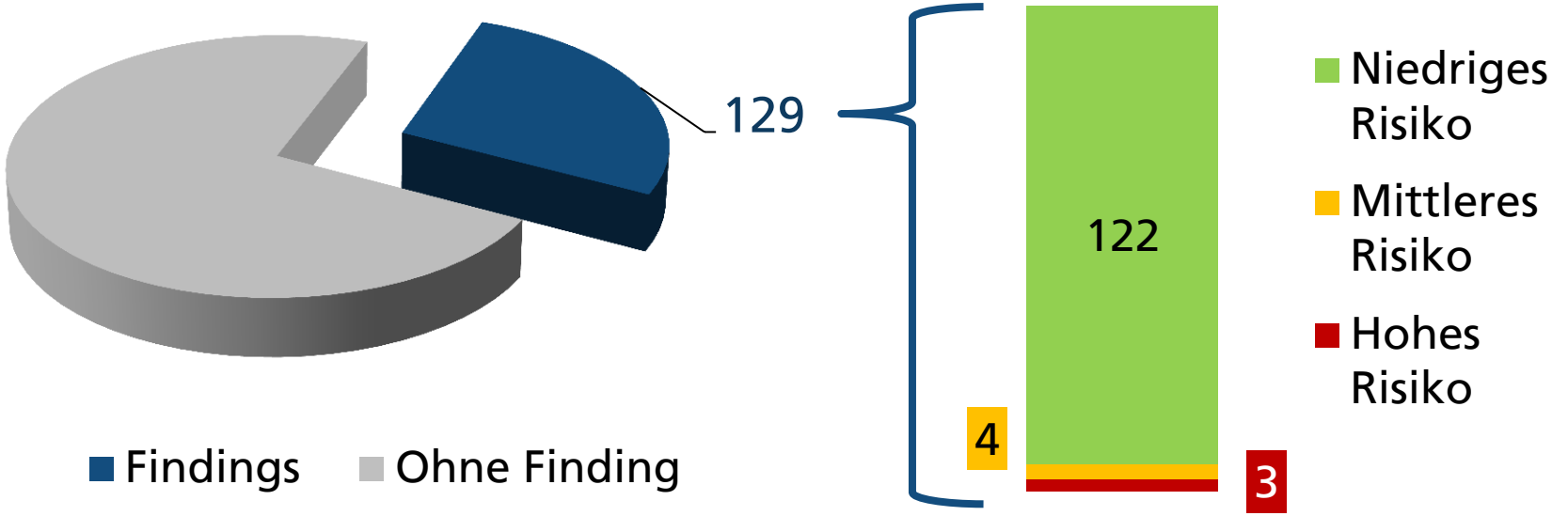
Götz Weinmann (IT-Security Consultant)

1. Juni 2015

Management Summary

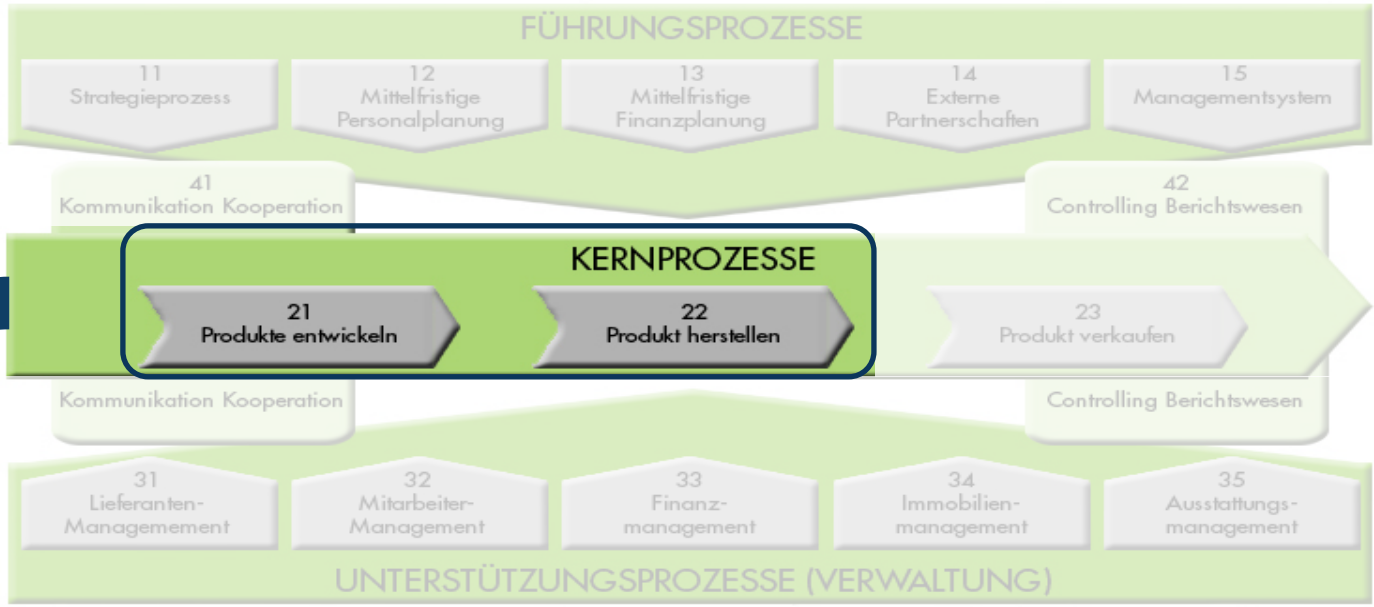
- Im Rahmen eines richtlinienbasierten Security Audits wurden zwei **Server** aus den Bereichen **Entwicklung** sowie **Produktion** auf sicherheitsrelevante Einstellungen, Konfigurationen und Softwareversionen hin untersucht.

Ergebnis bei 474 relevanten Richtlinien:



Auswahl der Systeme

- Die Kernprozesse und die relevanten, beteiligten Systeme wurden anhand der vorhandenen Prozesslandkarte festgelegt



Der Entwicklungsprozess wird durch SERVER1, der Produktionsprozess durch SERVER2 unterstützt.

High Risk Findings

- Die Bewertung der Findings erfolgt auf Basis einer Risikoeinschätzung.
  Faktoren: Auswirkung bei Eintritt, Wahrscheinlichkeit des Eintritts.

Richtlinie: PS-SYS1 - 7.1 Allgemeine Vorgaben

- In der $PATH-Variable darf der "." nicht enthalten sein.

Empfehlung:

- Die Richtlinie sollte unbedingt umgesetzt werden. Begründungen für Ausnahmen sind nicht erkennbar.

Wurde im Rahmen des Audits an allen betroffenen Servern umgesetzt.

➔ Bewertung: 

High Risk Findings

Richtlinie: BSI IT GS - Netzwerk

- Server mit hohem Schutzbedarf sollten in logisch getrennten Netzwerkbereichen stehen.

Empfehlung:

- Da die vorhandene Infrastruktur eine Umsetzung leicht ermöglicht (Core-Switch), wird dringend empfohlen, dass das System in einem durch eine Firewall abgeschotteten Bereich (Separate Zone) vom restlichen Netzwerk getrennt wird.

➔ Bewertung: 

Medium Risk Findings

Richtlinie: PS-SYS17- 8.2 Login Policy

- Automatischer Logout nach 3 Minuten Inaktivität muss eingerichtet sein.

Empfehlung:

- Die Richtlinie sollte unbedingt umgesetzt werden. Begründungen für Ausnahmen sind nicht erkennbar.

➔ Bewertung: 

Wurde im Rahmen des Audits an allen betroffenen Servern umgesetzt.

Medium Risk Findings

Richtlinie: PS-SYS17- 9.8 Syslog

- Die Speicherung der Logdaten auf einen zentralen Logserver ist empfehlenswert.

Empfehlung:

- Die Richtlinie sollte unbedingt umgesetzt werden. Begründungen für Ausnahmen sind nicht erkennbar.

➔ Bewertung: 

Fazit

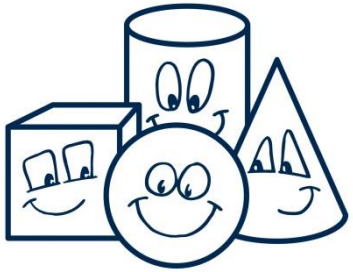
- Die beanstandeten Findings können mit wenigen Ausnahmen schnell durch **Konfigurationsänderungen** oder **Softwareupdates** abgeschaltet werden.

- Die Findings der Prio **HIGH** Risk wurden im Rahmen des Audits **beseitigt**. (Ausnahme: Netzwerkanbindung SERVER1).

- Es wird dringend empfohlen, Server mit hohem Schutzbedarf in logisch **getrennten Netzwerkbereichen** zu implementieren.

- Es wird empfohlen eine **zentrale Log-Server Plattform** inklusive Management einzuführen. So können sicherheits-relevante Systemkonfigurationen an zentraler Stelle abgebildet werden. Im Falle eines Sicherheitsvorfalls kann so der Angriff besser nachvollzogen werden.

MUSTER / AUSZUG
Präsentation Ergebnisbericht
TOsecurity Audit



Fragen?

Götz Weinmann
IT-Security Consultant
TOsecurity

Tel. +49 711 88770-xxx
yyyyy.zzzzzzzzzzz@to.com

Michael Schrenk
Bereichsleitung
Vertrieb & Marketing

Tel. +49 711 88770-xxx
yyyyy.zzzzzzzzzzz@to.com

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal / Stuttgart

Tel. +49 711 88770400
Fax +49 711 88770449
www.to.com