

VIRTUAL FORGE

5 Wege, Ihr SAP System
anzugreifen

Patrick Boch, 5. Juni 2018

Führender Hersteller von Cyber-Sicherheitslösungen für SAP

<p>Nachhaltiges Wachstum seit 2001</p> 	<p>100+ Experten weltweit</p> <p>200+ Zufriedene Kunden</p>			<p>Erfinder des ABAP und HANA Code Scanners</p> <p>Patentgeschützte Lösungen</p>
		<p>SAP-Sicherheit ist unsere Mission!</p>	 <p>SAP® Certified Integration with SAP Applications</p> <p>SAP® Certified Powered by SAP NetWeaver®</p>	<p>USA Spanien Niederlande Deutschland (HQ) Singapur UAE GB</p>

01

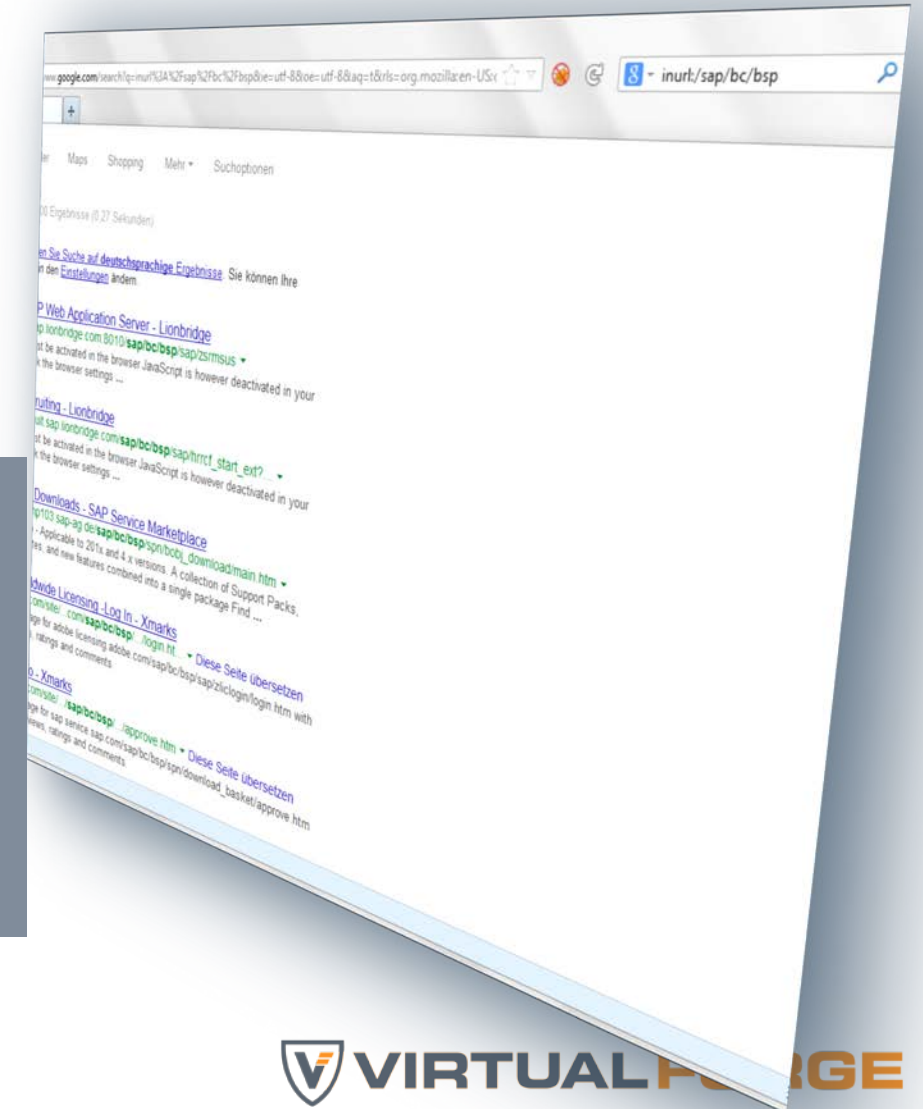
5 WEGE, IHR SAP SYSTEM ANZUGREIFEN

#1 Der Einfache Weg

- SAP Systeme können einfach im Internet gefunden werden
- Unberechtigter Zugriff möglich

Praktisches Beispiel:

- ✓ System über das Internet erreichbar (eRecruiting, Supplier Portal)
- ✓ SAP* nicht geändert
- ✓ Voller Zugriff über User SAP*, Passwort „PASS“

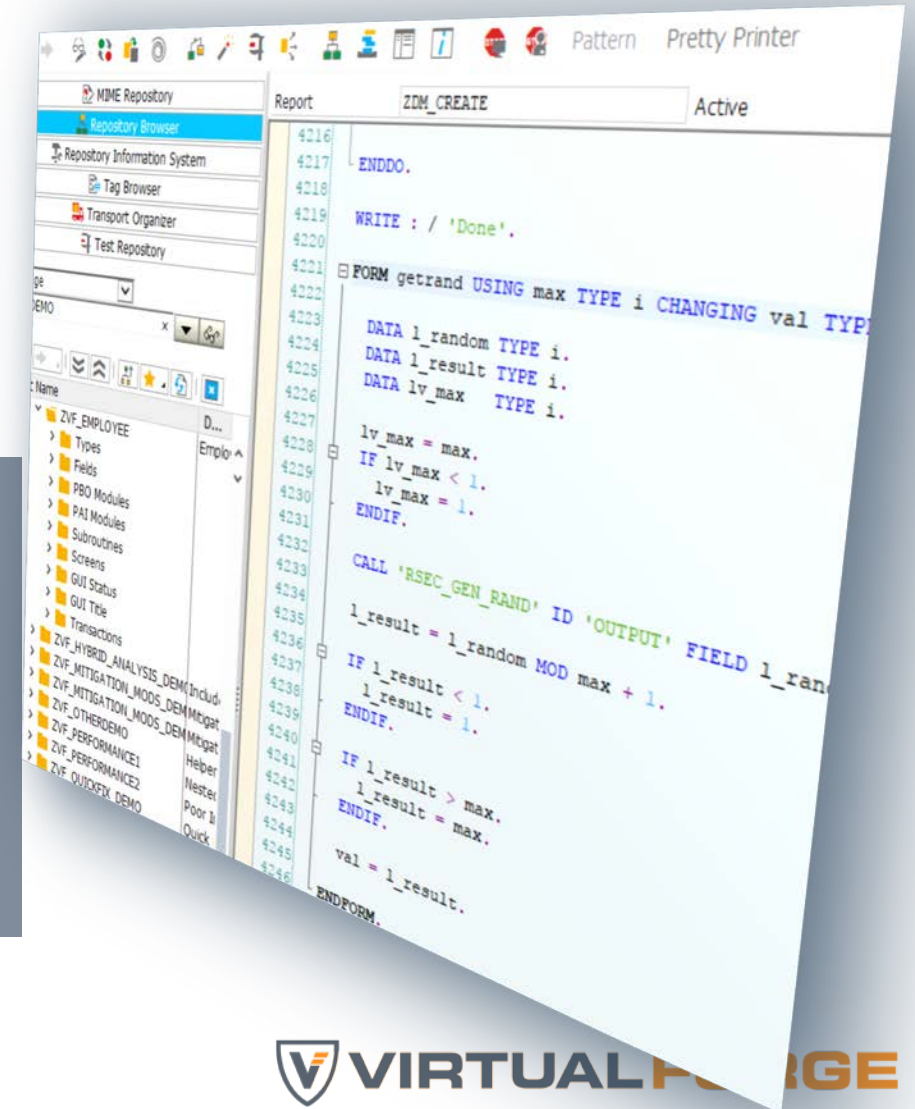


#2 Der böswillige Insider

- SAP Nutzer können recht einfach eine Hintertür öffnen und ausnutzen
- Funktioniert mit (beinahe) jedem SAP User

Praktisches Beispiel:

- ✓ Gmail-Adresse im ABAP Code versteckt
- ✓ Quartalsergebnisse 2-3 Tage vor Quartalsende per E-Mail verschickt
- ✓ Mitarbeiter seit 3 Jahren nicht mehr im Unternehmen



```
4216  
4217 - ENDDO.  
4218  
4219 WRITE : / 'Done'.  
4220  
4221 FORM getrand USING max TYPE i CHANGING val TYPE i  
4222  
4223 DATA l_random TYPE i.  
4224 DATA l_result TYPE i.  
4225 DATA lv_max TYPE i.  
4226  
4227 lv_max = max.  
4228 IF lv_max < 1.  
4229 lv_max = 1.  
4230 ENDIF.  
4231  
4232 CALL 'RSEC_GEN_RAND' ID 'OUTPUT' FIELD l_random  
4233  
4234 l_result = l_random MOD max + 1.  
4235  
4236 IF l_result < 1.  
4237 l_result = 1.  
4238 ENDIF.  
4239  
4240 IF l_result > max.  
4241 l_result = max.  
4242 ENDIF.  
4243  
4244 val = l_result.  
4245  
4246 ENDFORM.
```

#3 Der Hacker

- „Viele Wege führen nach Rom“ – bekannte Schwachstellen mittels Hard/Software ausnutzen
- Kein spezielles Wissen benötigt

Praktisches Beispiel:

- ✓ Wifi-Pineapple: einfach im Netz kaufen
- ✓ “Appstore” im Lieferumfang
- ✓ Ab in den nächsten Starbucks...



#4 Der Effektivste Weg

- Social Engineering – Die clevere Manipulation der menschlichen Tendenz, Vertrauen zu schenken
- Die wohl effektivste Art zu hacken

Praktisches Beispiel:

- ✓ Zufällige Nummern anrufen und vorgeben, im IT Support zu arbeiten
- ✓ Irgendwann fällt jemand drauf rein...

Kevin 'don't call me a security expert' Mitnick

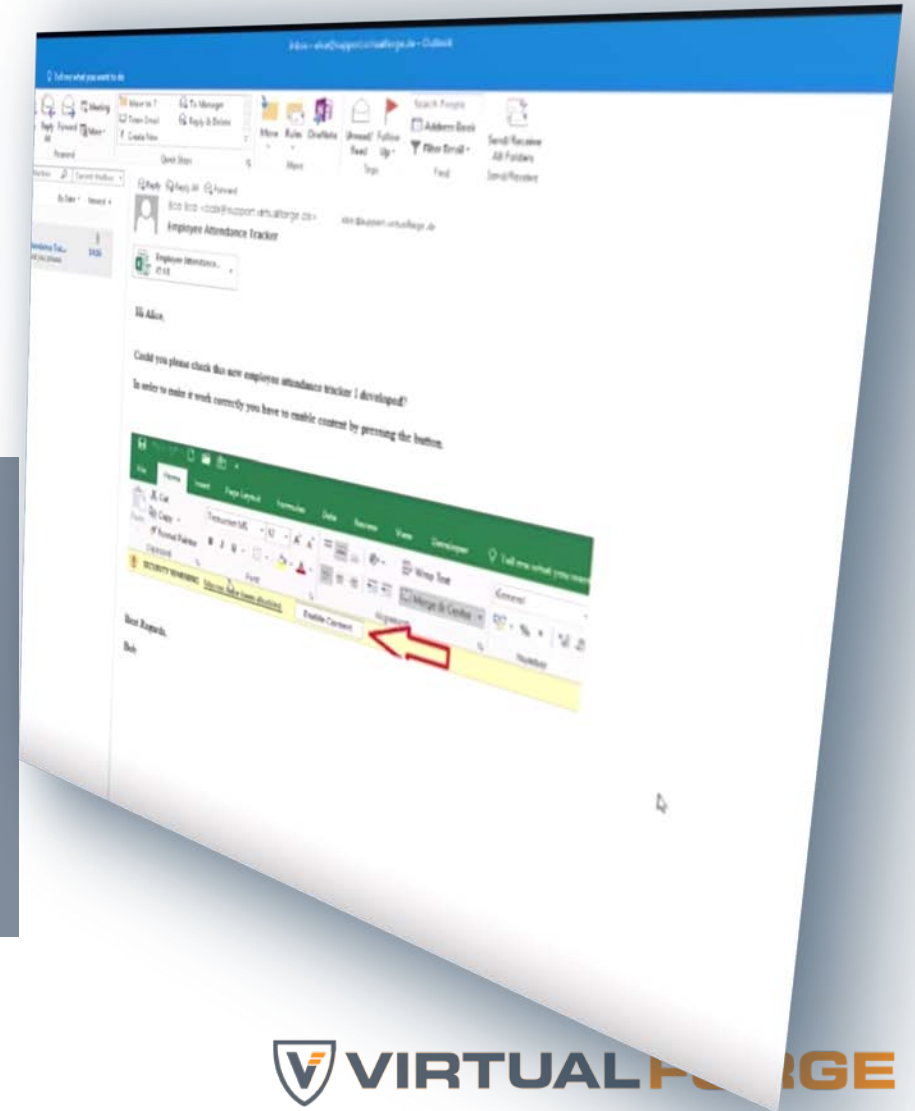


#5 Der Häufigste Weg

- Betrügerische Erhebung privater Informationen
- Normalerweise mittels Links zu Webseiten oder angehängten, schadhaften Dateien

Praktisches Beispiel:

- ✓ Spear Phishing – zielgerichtet auf bestimmte Person(en)
- ✓ Excel mit Makro um SAP_ALL zu erlangen



02

SAP SYSTEME ABSICHERN

SAP ist mehr als „nur“ eine Anwendung

SAP



Risiko-
Erkennung



Identity
Management



Infrastruktur



Konfiguration



Authentifizierung



Sichere
Entwicklung

SAP Security Management



Understand Your Risk

- Sicherheitsanforderungen identifizieren
- Schwachstellen analysieren

Get Clean

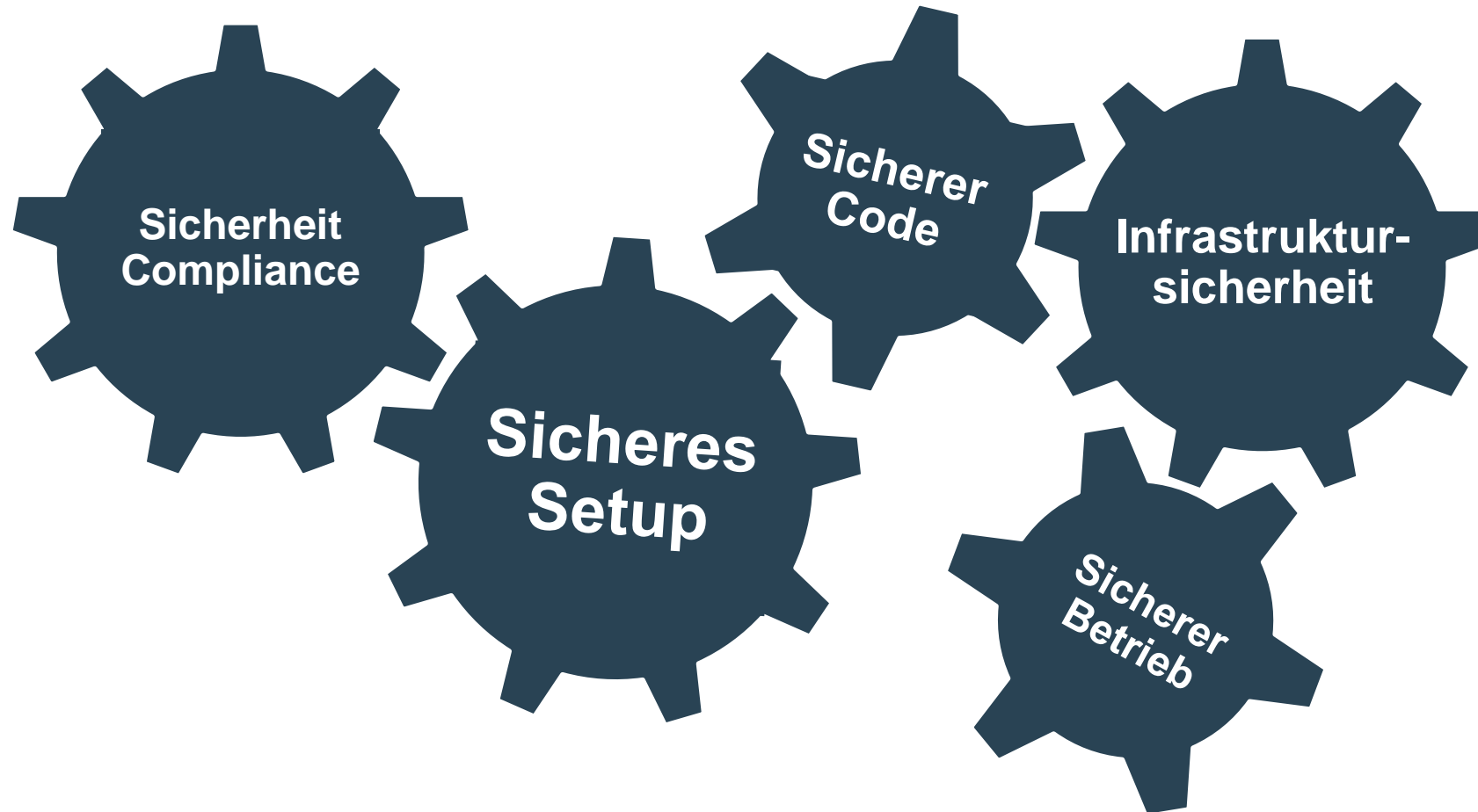
- Systeme absichern
- Schwachstellen beseitigen

Stay Clean

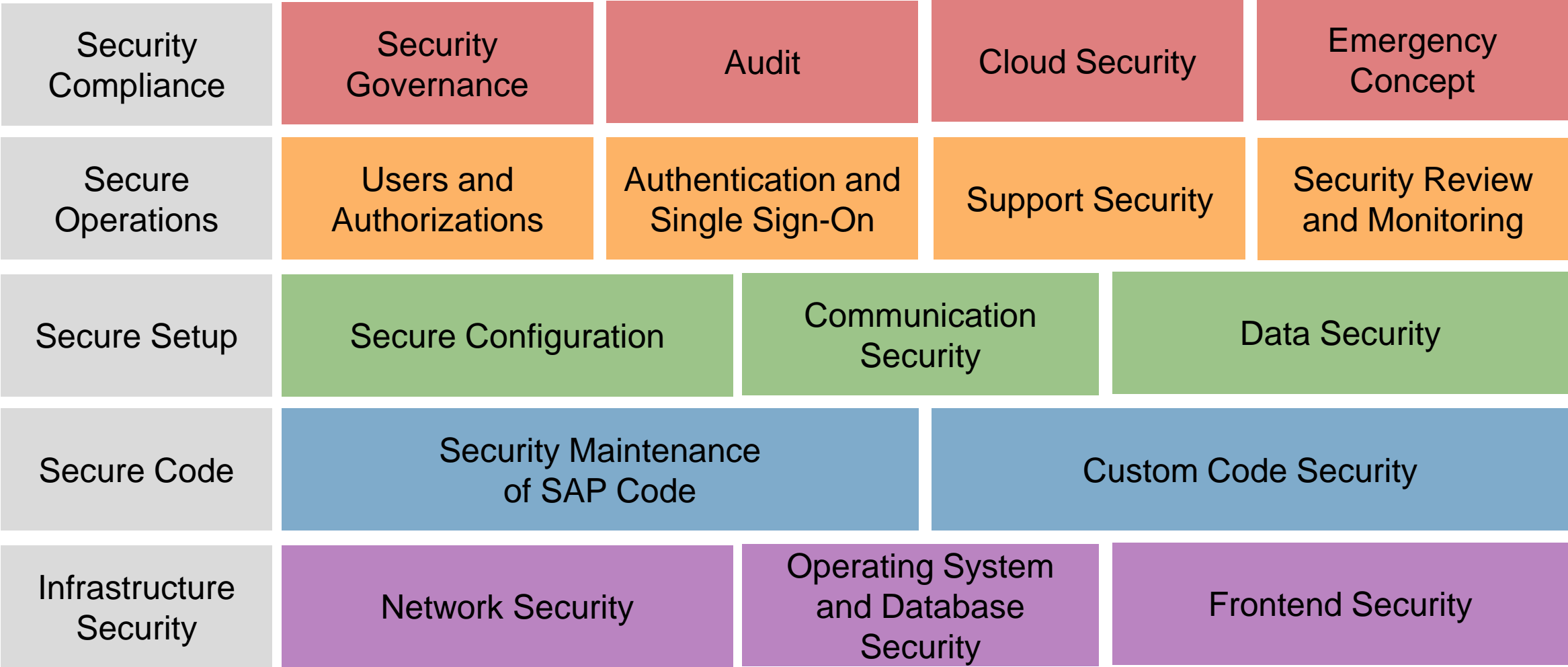
- Sicherheitskonzept umsetzen
- Systeme überwachen

Ganzheitliche Sicht auf SAP Security

SAP Secure Operations Map



SAP SECURE OPERATIONS MAP



Reference: SAP Security Baseline Template v 1.9 - SAP OSS Note 2253549



SAP Security Baseline Template



Security Compliance

- Einschränkung der Privilegien für Standardbenutzer, funktionale und technische Benutzer, Standardprofile, RFC-Berechtigungen und Remote-Zugriff
- Implementierung von Notfallplänen und Wiederherstellungs-/Business-Continuity-Plänen
- End-to-End-Verschlüsselung und sichere Nutzung der Kryptographie sicherstellen

SAP Security Baseline Template



Secure Setup

- Sicherheitspatches frühzeitig und regelmäßig implementieren
- Überwachung von Sicherheitseinstellungen und -parametern auf allen Systemen
- Sichere Kommunikation über RFC und Schnittstellen
- Implementierung von SAP SNC für ein sicheres Netzwerk

SAP Security Baseline Template



Secure Operations

- Kontinuierliche Systemüberwachung und -protokollierung
- Warnungen über Vorfälle und Reaktionen auf verdächtige Systemaktivitäten automatisieren
- Implementierung eines Life-Cycle-Management von Benutzerkonten und Systemzugriffen.
- Änderungen auf Risiken überprüfen vor dem Import in das Produktivsystem

SAP Security Baseline Template



Secure Code

- Etablierung und Durchsetzung von Entwicklungsstandards
- Implementierung eines sicheren Software Development Lifecycle mit Code-Scannern
- Frühes Scannen, häufiges Scannen - alle benutzerdefinierten und 3rd-Party-Codes
- Fehler risikobasiert korrigieren

SAP Security Baseline Template



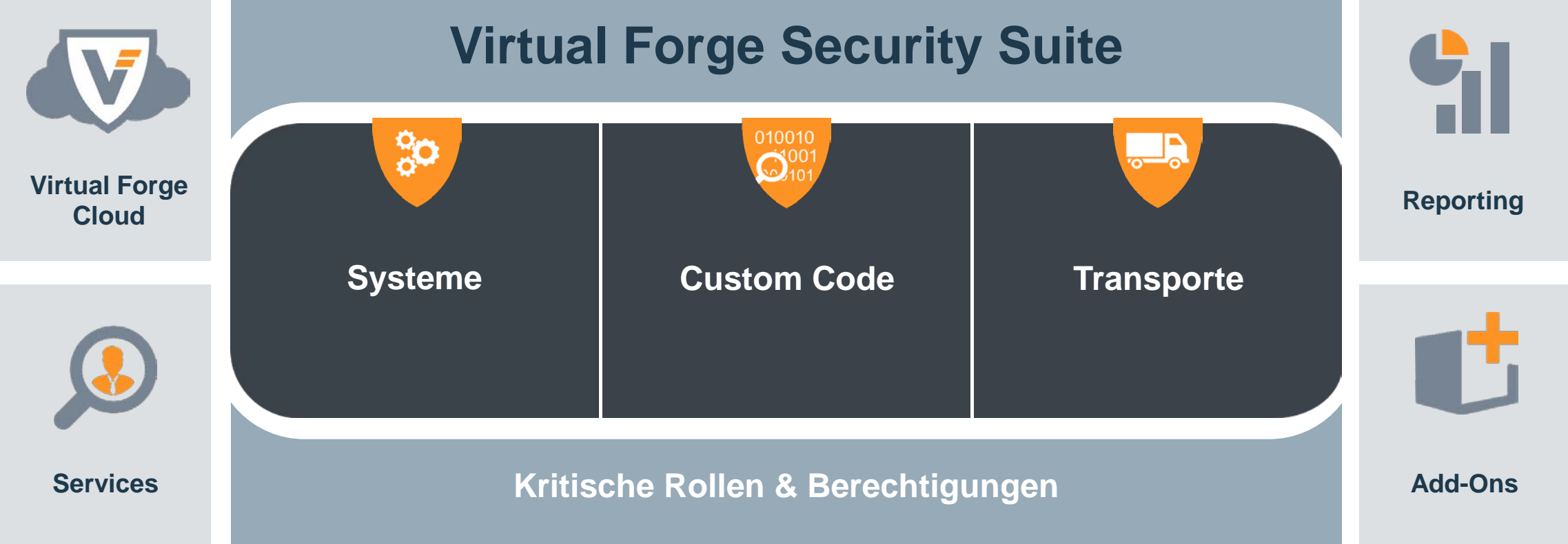
Infrastructure Security

- Analyse und Inventarisierung von SAP-Systemen, SAP-Servern, Geschäftsprozessen und Datenaustausch innerhalb der IT-Infrastruktur.
- RFCs steuern, SAP Router, SAP Web Dispatcher, SAP Gateway,....
- Patch und Update OS und DB
- Verwendung von sicheren OS/DB-Passwörter

03

SAP SECURITY LÖSUNGEN

Virtual Forge Portfolio



SERVICES



Understand Your Risk

- Schwachstellenanalysen
- Penetrationstests
- Audits
- Security Roadmap

Get Clean

- Implementierungs-Services
- Custom Code Correction Factory
- Secure Gateway Konfigurationen

Stay Clean

- Secure Patch Service / Secure Advisory Service
- Threat Monitoring Advisory

SAP Schwachstellenanalyse

Understand your Risk

Ganzheitliche Sicherheitsüberprüfung
eines Systems in den Bereichen
System, Code und Transporte



Analyse und Präsentation der Ergebnisse
durch erfahrene SAP Sicherheitsberater



Darstellung der gefundenen Schwachstellen
in einem übersichtlichen PDF Report



© 2018 Virtual Forge GmbH. All rights reserved.

Information contained in this publication is subject to change without prior notice. These materials are provided by Virtual Forge and serve only as information.

SAP, ABAP and other named SAP products and services as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries worldwide.

All other names of products and services are trademarks of their respective companies.

Virtual Forge accepts no liability or responsibility for errors or omissions in this publication. From the information contained in this publication, no further liability is assumed. No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Virtual Forge GmbH, Germany or Virtual Forge Inc. The General Terms and Conditions of Virtual Forge apply.