nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Workshop Risikomanagement

Impuls Vortrag

IT-Risiken Cyber Play GmbH

29. April 2015

Stephan Sachweh

Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen

pallas

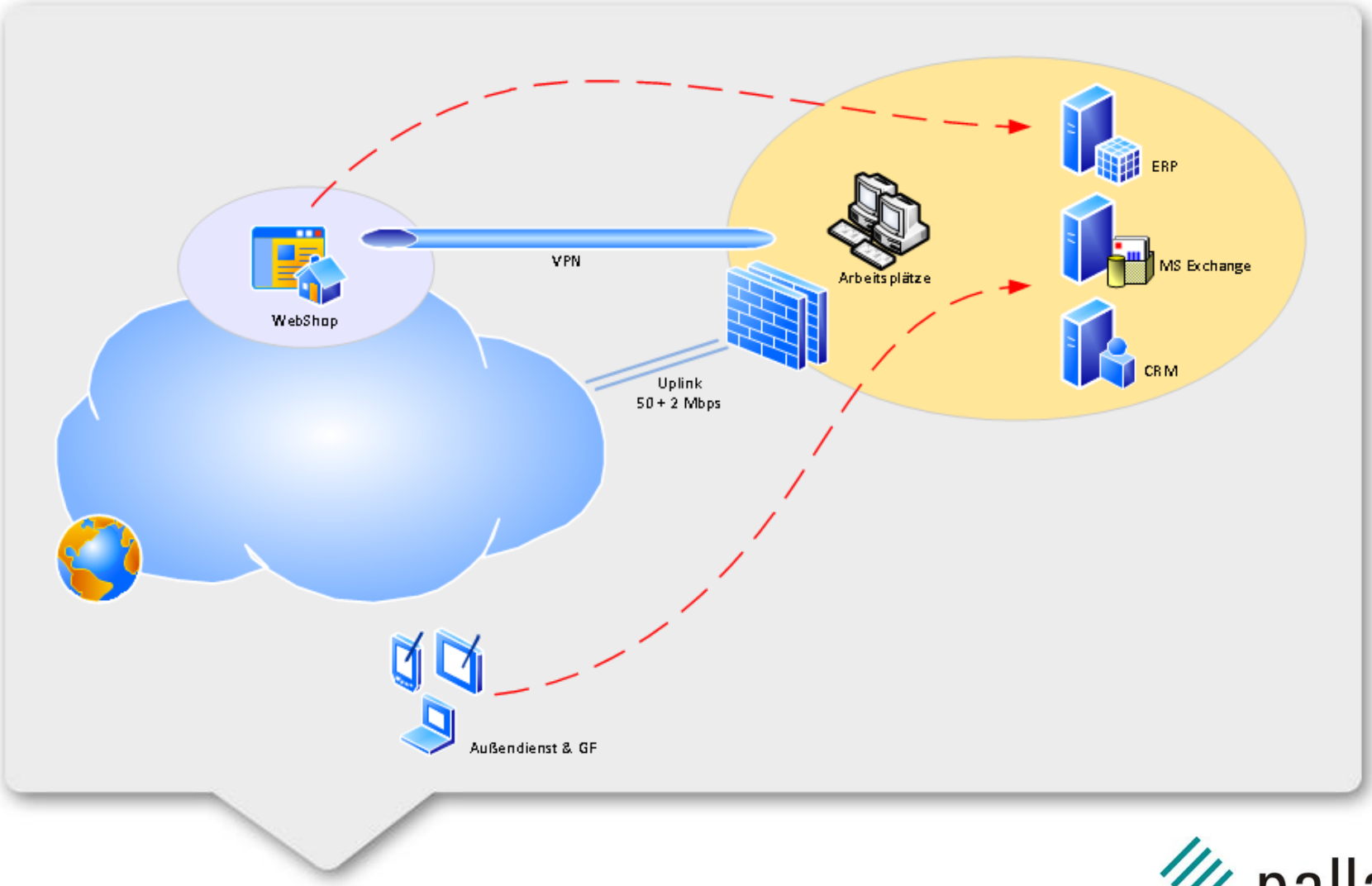
EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

Aspekte der IT-Risiken

- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Technik
- Organisation
- Verträge / Recht

- Typische Probleme
  - Fokussierung auf Teilaspekt
  - „Eingeschränkte" Experten-Sicht
  - Kein angeborenes „Gefühl" für Wahrscheinlichkeiten
  - Unnötige Tendenz zum Zero-Risk
  - Suche meist nur nach technischen Lösungen

IT-Landschaft Cyber Play GmbH



Risiken ERP der Cyber Play GmbH

- Kern-System („Kronjuwel“)
  - Enthält u.a. Stücklisten & Bauanleitungen für Produktion, Lieferanten, EKs, Rahmenverträge und kundenspez. VKs
- Kein Warenein- und -ausgang ohne ERP
- Know-How zu ERP auf wenige (zwei) internen Mitarbeiter verteilt
- Keine Hochverfügbarkeit aufgrund von Lizenzkosten und Komplexität
- Gefahr ungepatches Betriebssystem
- Nicht Erreichbarkeit durch Ausfall WAN
- Keine Rechtebegrenzung auf Datenbank-Ebene
- Gefahr Starkregen (→ Server-Raum im UG)

Risiken Web-Shop

- Unzureichende SLA-Regelungen / Pönalen
- Nichterfüllung PCI-DSS
- Ausfall durch vorgelagerte, singuläre Systeme trotz Hochverfügbarkeit Web-Server
- Mangelhafte Konfiguration Web-Server / Datenbank
- Gefahr Customized Standard-Software
  - Alte, unsichere Version, da nicht Update-fähig
  - Abhängigkeit Web-Designer / Programmierer
- Manipulation und Ausfall durch Angriffe
  - XSS, SQLi, Session-Diebstahl, DDoS, …
- Ausfall durch Backend Abhängigkeit ERP

Risiken Organisation

- Kein Bewusstsein Gesamtverantwortung der GF für IT-Sicherheit
- Kein IT-Sicherheitsbeauftragter/Sicherheitsgremium
- Keine Vorgaben zum Umgang mit Passwörtern
- Bestehender Outsourcing Vertrag zur *IT-Super AG*
  - Eigene Sicherheitsstandards nicht berücksichtigt
  - Keine ausreichende Protokollierung bei Fernwartung
  - Keine namentliche Nennung und Verpflichtung zur Verschwiegenheit der Entwickler/Supportler mit ERP-Zugriff
- Kein Notfallplan
- Keine regelmäßigen Test-Recovery‘s aus dem Backup
- Netzwerkschränke mit Standard-Hersteller-Schlüssel

Stay secure …

- Schützen Sie primär Ihre „Kronjuwelen“
- Sensibilisieren und schulen Sie Ihre Mitarbeiter
- Bewerten und dokumentieren Sie Ihre IT-Risiken
- Akzeptieren Sie Ihre Restrisiken
- Nehmen Sie verschiedene Sichtweisen ein