UMSTIEG IN DIE CLOUD... *mit Sicherheit*

TEIL 2 VON 3

AUS DEM INHALT

5 NETZWERK

Da die Verantwortung zum Betrieb im eigenen Unternehmen verbleibt, muss klar sein, dass der Punkt „Netzwerke“ ein zukünftig wichtiger Punkt der Betrachtung ist. Die Schlüsselfrage in diesem Bereich der Netzwerke heißt:

“Inwieweit sind Daten im Rahmen der Transporte durch die Cloud, z.B. durch Verschlüsselung (z.B. SSL, TLS, …), gegen Einsichtnahme gesichert?“

Wer benötigt und hat tatsächlich einen Zugriff auf die Konfiguration und Änderung der VPN-Einstellungen sowie die Fragestellung “Kann ich mit z.B. unternehmenseigenen Zertifikaten arbeiten oder ist es erforderlich und sind Risiken tragbar in dem Wissen, dass der Provider selbst die Konfiguration und Daten einsehen kann?“

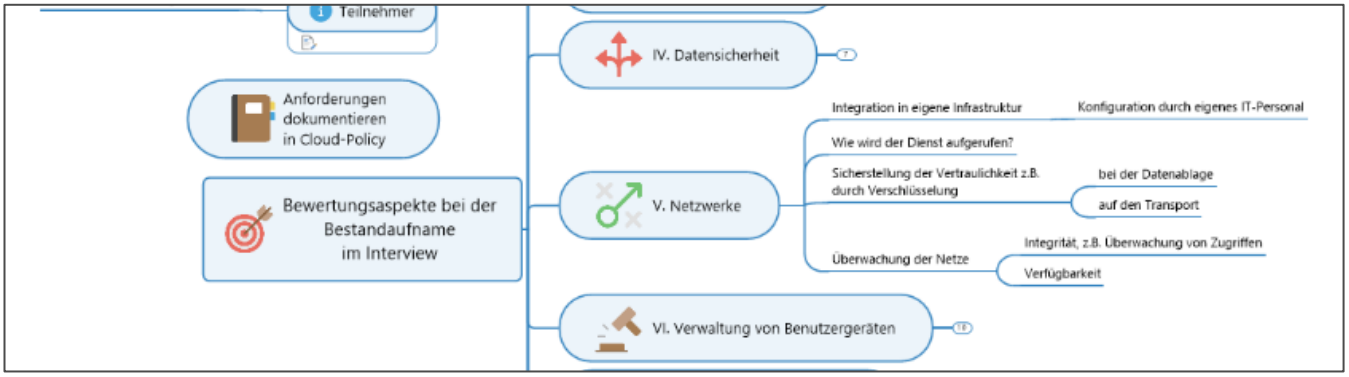

Abbildung 1 Netzwerk

Mögliche Kontrollfragen können hier sein:

- Sind die Anforderungen, die seitens der eigenen Organisation und auch der eigenen Kunden an den Schutz von Informationen gestellt werden, ausreichend verstanden und umgesetzt, z.B. die Segmentierung?
- Reichen die angebotenen Möglichkeiten der Dienste aus bzw. sind zusätzliche Schutzmaßnahmen erforderlich (Zugriff nur über unternehmenseigenes VPN etc.)?
- Kann eigenen Mitarbeitern und auch Administratoren auch im Notfall ein Zugriff auf die Dienste ermöglicht werden (Fernzugriff, Internet- oder VPN-Zugriff)?
- Werden Schutzmaßnahmen permanent überprüft und ggf. nachjustiert und durch wen? Wer ist für die Verwaltung der Firewalls verantwortlich?
- Sind die Hauptverkehrswege im Netzwerk geschützt und/ oder alle möglichen Routen zum virtuellen Netzwerk abgedeckt?
- Können ihre virtuellen Netzwerkressourcen im Falle einer erhöhten Belastung des Netzwerkverkehrs skaliert werden?

6 VERWALTUNG VON BENUTZERGERÄTEN

Für jeden zu verwenden Dienst ist es im Vorfeld unabdingbar zu ermitteln, wie die genaue Ein- oder Anbindung an die für die Nutzung erforderlichen Datenendgeräte (PCs, Smartphones, Tablets, etc.) gestaltet werden muss und welche Mindestvoraussetzungen gelten. Das Spektrum der zu betrachtenden Punkte ist hier umfangreich und muss unternehmensindividuell erfolgen. Die Einführung einer z.B. Mehrfaktorauthentifizierung über ein Smartphone ist nur praktikabel, wenn die benötigten Mitarbeiter entsprechende Smartphones besitzen, die ihrerseits durch ein zeitgemäßes Mobile Device Management abgesichert sind. Zusätzlich muss ermittelt werden, welche Risiken vertraglich abgesichert sind (z.B. im Falle von Zugriffen durch den Provider selbst).

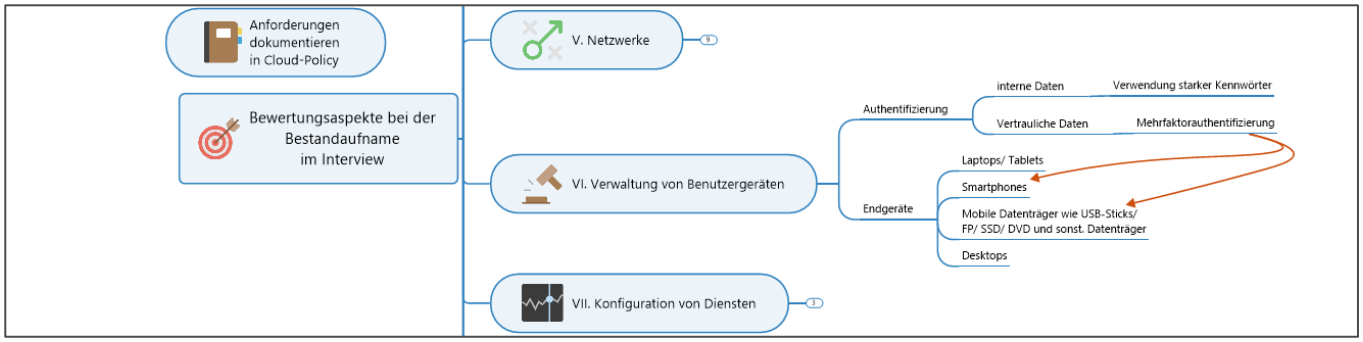

Abbildung 2 Verwaltung von Benutzergeräten

Mögliche Kontrollfragen können hier sein:

- Ist der Workflow zwischen Benutzergerät und Netzwerkkonstrukt bekannt?
- Verfügen Sie über ein Verwaltungsprofil auf den mobilen Geräten der Benutzer?
- Wie werden Benutzergeräte verwaltet?
- Wer sorgt für erforderliche Betriebssystemaktualisierungen und wie?

7 KONFIGURATION VON DIENSTEN

Für den Einsatz unternehmensfremder Dienste ist es von entscheidender Bedeutung, welche Möglichkeiten und Anpassungen zukünftig in der eigenen Konfiguration der Dienste noch möglich sind. In diesem Zusammenhang erörtert sich gleichfalls die Frage der zukünftigen Verantwortung, die sorgfältig in den Verträgen ausreichend und rechtsverbindlich vereinbart werden.

Zusätzlich ist es wichtig, sowohl die eigenen als auch die fremden Verantwortungen genau abzugrenzen, festzulegen und dieses für alle Beteiligten rechtsverbindlich zu dokumentieren (z.B. SLAs, OLAs, interne Regelungen…). Voraussetzung hierfür ist, die verwendeten Dienste ausreichend zu verstehen.

Abbildung 3 Konfiguration von Diensten

Mögliche Kontrollfragen können hier sein:

- Für welche Teile des Konfigurationsmanagements ist die eigene Organisation zuständig und verantwortlich? Welche Teile werden zukünftig durch den Diensteanbieter verwaltet und durchgeführt?
- Reicht der eigene Zugriff aus, um die Anforderungen der Organisation an Vertraulichkeit, Integrität und Verfügbarkeit auch zukünftig sicher zu stellen?
- Sind die zu betrachtenden relevanten Konfigurationen auch ausreichend bekannt, dokumentiert und sind Mitarbeiter für die Aufgaben ausreichend geschult?
- Welche Risiken ergeben sich für die eigene Organisation, wenn sich die Umgebung beim Service-Provider, z.B. durch Weiterentwicklung, ändert?
- Sind entsprechende Möglichkeiten mittels Standardschnittstellen ausreichend betrachtet, die auch später einen Wechsel des Serviceproviders erheblich vereinfachen können?

8 SCHWACHSTELLEN-MANAGEMENT

Im Rahmen des Schwachstellen-Managements bieten viele etablierte Diensteanbieter professionelle und effektive Lösungen an, die dem eigenen Schwachstellen-Management erheblich überlegen sind, da sie z.B. durch den Diensteanbieter selber aus erster Hand durchgeführt werden können (beispielsweise Microsoft Azure). So kann ein Teil des Patchmanagement häufig als zusätzlicher Vorteil an den Diensteanbieter ausgelagert werden. Trotzdem ist es unerlässlich, genauer in den Verträgen zu prüfen und im Vorfeld sicherzustellen, dass ein ausreichendes Schnittstellenmanagement gewährleistet ist.

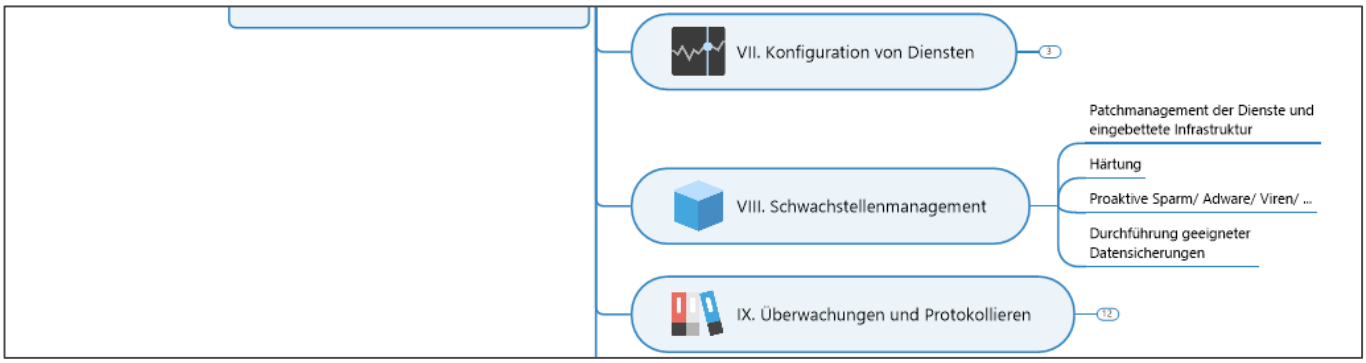

Abbildung 4 Schwachstellenmanagement

Mögliche Kontrollfragen können hier sein:

- Sind die relevanten Risiken durch Schäden eines unzureichenden Patch-Managements ermittelt?
- Wofür wird der Cloud-Dienst originär verwendet (Speicherung, finanzielle Transaktionen etc.) und welche Anforderungen bestehen seitens der Verfügbarkeit und Integrität an Dienste und Daten?
- Wie lange wird ein Ausfall des Dienstes tatsächlich verkraftet (z.B. E-Mail, Datenablage, Zahlungsdienste, Rechnungsschreibung, Web-Shops etc.)?
- Welche konkreten Prozesse, Werkzeuge und welche Vorgehensweise zur Ermittlung von Schwachstellen werden vom Anbieter verwendet und welche Kontrollen bestehen?
- Wie stellt sich das Schwachstellenmanagement bezüglich der Kontrolle, proaktiver Erkennung, Virus-Erkennung (z.B. Ransom) dar? Wo liegen die Grenzen (z.B. bei der Erkennung von Phishing-Mails)?
- Wie sind die Systeme des Anbieters gehärtet?
- Werden Sie über Updates informiert, die z.B. auch in der Konsequenz dazu führen, dass eigene Systeme zusätzliche Bedeutung erhalten, z.B. in der Industrie?
- Erfolgt die regelmäßige Überprüfung mittels Penetrationstests?

Fortsetzung des Fachbeitrages mit Teil 3 in Folge 10…

Der Autor Bernd Schart ist seit 2009 Mitarbeiter der OS und beschäftigt sich im Fachgebiet Security & Audit seit 2011 als Auditor mit dem Thema Informationssicherheit in der Automobilindustrie. Bernd Schart betreibt seit 2020 einen eigenen, freien und unabhängigen Podcast (WWW.ISITALK.DE) zu Themen der Informationssicherheit, speziell auch den Anforderungen des VDA ISA im Rahmen von TISAX® Assessments.